

**ATTACHMENT A**

**CONTRACT**

**FOR**

**Kentucky Department of Education  
K-12 Schools Connected User Experience (CUES)**

**BETWEEN**

**THE COMMONWEALTH OF KENTUCKY**

**Finance and Administration Cabinet  
On Behalf of  
Kentucky Department of Education (KDE)**

**AND**

**Identity Automation LP**

**MA 758 2400000661**

**VENDOR CONTACT INFORMATION:**

**Carter Dunbar  
7102 N. Sam Houston Pkwy, West, Suite 100  
Houston, TX 77064  
cdunbar@identityautomation.com  
(817) 937-7785**

**PROGRAMMATIC QUESTIONS/ISSUES MUST BE DIRECTED TO THE AGENCY  
CONTACT(S).**

**AGENCY CONTACT INFORMATION:**

**Name: Mike Leadingham  
Email: [Mike.Leamingham@education.ky.gov](mailto:Mike.Leamingham@education.ky.gov)  
Phone:502-564-2020 x2202**

**AGENCY PROCUREMENT CONTACT:**

**Name: Raven Miller  
Email: [Raven.Miller@education.ky.gov](mailto:Raven.Miller@education.ky.gov)**

Phone: (502) 564-1979 ext. 4345

**CONTRACTUAL QUESTIONS/ISSUES MUST BE DIRECTED TO THE OFFICE OF  
PROCUREMENT SERVICES CONTACT.**

**OFFICE OF PROCUREMENT SERVICES CONTACT INFORMATION:**

**Name: Susan S. Noland, KCPM**

**Email: Susan.Noland@ky.gov**

**Phone: (502) 564-5951**

\*\*\*\*\*

This Master Agreement (“Contract”, “Award” or “Agreement”) is entered into, by and between the Commonwealth of Kentucky, **Kentucky Department of Education** (“the Commonwealth”, “Customer” or “KDE”) and **Identity Automation LP** (“Contractor”, “Vendor” or “IA”) as the Prime Vendor.

The Commonwealth and Contractor agree to the following:

**I. Scope of Contract**

The purpose of this Contract will provide a vendor managed, industry recognized, K-12-centric, full-featured Software as a Service (SaaS) identity management (IdM) solution as a state education agency (SEA) funded, statewide shared service. This resulting service will establish a single, secure, cloud-based identity for all K-12 students, teachers, and staff, and leverage and securely integrate (and interoperate) the statewide standardized student information system (SIS) and standardized financial management application (ERP/HR) with the variety of education-specific cloud-based ecosystems and services for all 177 sites (*See Attachment C: Connected User Experience System Site List*).

**II. Negotiated Items**

1. Identity Automation shall host the CUES platform in a cloud-based secure, reliable redundant datacenter, AWS.
2. Addition of Section 10.32 – Insurance Requirements
3. The Commonwealth/KDE reserves the right to add the Value Added Service “Security Manager” at a rate not to exceed \$6.00 per full time employee count of the LEA (Local Education Agency) and KDE Annually – Price Locked for the Contract Term.
4. The Commonwealth/KDE reserves the right to add the Value Added Service “PhishID” at a rate not to exceed \$0.87 per user, which includes Staff and Student Count of the LEA (Local Education Agency) and KDE Annually – Price Locked for the Contract Term
5. The Commonwealth/KDE and Identity Automation will finalize the Service Level Agreement after contract award.

6. District Engagement – Identity Automation shall provide, engage and guide each district on an individual bases, according to the LEA’s capabilities and maturity to ensure success.
7. Pricing – Payment Schedule – See Section IV Pricing
8. Identity Automation confirms the following Rapid Identity IA Features and/or modules are included in Baseline Services:
  - Identity Lifecycle Management (User and Group Management)
  - Workflow (Governance)
  - Rostering (Class Roster Synching for K-12)
  - Authentication (MFA & SSO)
  - SafeID (Compromised Credential Monitoring)
  - ShieldID (Virtual Firewall & Geofencing)
9. Family Educational Rights and Privacy Act - If during the course of this Contract, KDE discloses to the contractor any data protected by the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended, and its regulations, and data protected by the Richard B. Russell National School Lunch Act (42 U.S.C. 1751 et seq) (NSLA) and Child Nutrition Act of 1966 (42 U.S.C. 1771 et seq.) (CNA) the contractor is bound by the confidentiality, security and redisclosure requirements and restrictions stated in FERPA, NSLA and CNA and will enter into a confidentiality agreement and ensure its employees and contractors execute affidavits of nondisclosure as required by KDE.
10. Student Data Security  
Pursuant to KRS 365.734 (House Bill 232 (2014)), if contractor is a known cloud computing service provider (as defined in KRS 365.734(1)(b) as “any person or entity other than an educational institution that operates cloud computing services”), or, through service to agency, becomes the equivalent of a cloud computing service provider, contractor does further agree that: Contractor shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student’s parent. The contractor shall work with the student’s school and district to determine the best method of collecting parental permission. KRS 365.734 defines “process” and “student data”. With a written agreement for educational research, contractor may assist an educational institution to conduct educational research as permitted by the Family Education Rights and Privacy Act of 1974, as amended, 20 U.S.C.sec.1232g. Pursuant to KRS 365.734, contractor shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes. Pursuant to KRS 365.734, contractor shall not sell, disclose, or otherwise process student data for any commercial purpose.  
Pursuant to KRS 365.734, contractor shall certify in writing to the agency that it will comply with KRS 365.734(2).
11. Identity Automation confirms no additional agreements or licenses required.

### III. Terms and Conditions

#### SECTION 3 – SCOPE OF WORK

##### 3.1 Scope of Work/Technical Requirements

The Kentucky Department of Education (KDE) recognizes that secure and straightforward user identity services are an essential element for providing instructional and support services to all K-12 Public School Districts, KDE, the Kentucky School for the Blind, and the Kentucky School for the Deaf (KSD). This Contract will provide Identity provisioning; age and ability appropriate platform-agnostic authentication; industry standard identity security functions and associated interrelated cloud-based managed services to all K-12 Public School Districts, KDE, the Kentucky School for the Blind (KSB), and the Kentucky School for the Deaf (KSD). A baseline level of these services is intended to be provided as a statewide shared service to all school districts and the KDE, with optional customizable services made available for implementation (including the potential for additional purchases beyond the baseline) by each district. Optional customizations by individual school districts shall fit within the statewide shared service model. The services provided by this Contract should be fully implemented and operational for all students, teachers, and staff within two years of the contract award.

##### A. General Requirements

###### 1. Account Team

The Commonwealth finds it crucial to have an account team identified and available with which to form a partnership. This mutual working partnership affords the vendor and Commonwealth insight and input into success measures, service evolution, and outcomes. The vendor shall provide an account team role (not necessarily titles) that includes, but is not limited to, an executive account representative, pre-sales engineer and a post-sales technical support manager that are based in the United States and are available for recurring meetings (at least quarterly after implementation).

- a. During implementation the Account Team shall provide a weekly services/project update.
- b. Post implementation, the Account Team shall participate in a monthly status/update meeting.
- c. The Account Team shall be prepared to work with districts (on enhanced functionality or customization) as well as with KDE.

###### 2. Engineering Assistance

- a. Vendor shall provide access to product and design engineers with expertise in implementing, managing, monitoring, and troubleshooting all services that are part of this Contract as implemented in Kentucky (i.e., identity provisioning from sources to relying parties, IdP SSO (MFA, SSPR, etc.), as well as product road mapping).
  - b. Vendor shall ensure that their engineering assistance, internal teams and/or subcontractors provide a coordinated engagement to KDE and K-12.
3. Vendor shall propose a fully managed service, in which the KDE and districts are not required to carry out technical administrative or operational tasks, monitor the health of any part of the service, or be solely responsible for detailed technical troubleshooting of the service.
4. Product Lifecycle  
Vendor shall have a product life cycle plan that includes communication to KDE and K-12 school districts with opportunities for customer product/service feedback. Customer product/service feedback should drive future improvements and features and prioritize the statewide shared service design needs and school districts and guide the work of vendor technical teams.
5. Baseline licensing and optional modules/services
  - a. Vendor shall provide implementation models including any costs associated with milestones, district training, customer education and training, etc.
  - b. Vendor shall provide an all-inclusive annual pricing model (one flat rate/Annual cost), which shall include Annual Enterprise licensing/Subscription/Service based on total K12 population (all staff, teachers, and students) and all associated annual costs (management, support, infrastructure hosting costs, ongoing professional development, etc.) for all identified sites. The proposed costs shall not assume that any existing districts using the solution continue to pay separately for the baseline functionality covered by this Contract, as the intent of the KDE is to pay for baseline functionality (as described elsewhere in this Contract) for all public-school districts. The vendor must include all sites in the total cost. Furthermore, the Commonwealth desires to not own, lease, or manage any technology assets associated with this service, and the submitted proposal must include all costs and fees associated with the solution.
  - c. Vendor shall allow for Extensibility and Customization for individual districts or on a statewide basis at either district or KDE expense with an equitable licensing/subscription model. For example, a district may wish to implement provisioning and/or authentication to a system that is only used by that district, or KDE may decide after contract signing

to implement provisioning and/or authentication for all districts to a system not already mentioned in this Contract.

- d. As enhanced or improved services within the general scope of this Contract become available, the vendor should make these services available on the Contract. These services shall meet industry-accepted standards for performance and operation and be equitably and competitively priced.
  - e. Vendor shall work with KDE and K-12 school districts to ensure that any federal or state statutory requirements can be met in a timely and efficient manner, including but not limited to language supports for limited English proficiency.
6. Section 508 Compliance
- All user interfaces to the solution(s) provided, shall be warranted by the vendor to comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG) 2.0, conformance level Double-A or greater.
7. Data Transition at End of Contract
- a. At the end of the contract, Vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The vendor shall cooperate to this end with the vendor of the agency's choice, in a timely and efficient manner.
  - b. At the end of the contract, Vendor shall destroy all Commonwealth data in its possession as defined in CIO-092 and provide a certification of the complete and permanent deletion of Commonwealth data.
8. Reliability
- a. Vendor's authentication system shall be designed to achieve at least 99.99% high-quality uptime from the perspective of end users. Uptime expectation excludes reasonable scheduled outages for upgrades, repairs, etc. as well as outages caused by factors outside of vendor control (such as KDE/school district network outages).
  - b. Vendor's provisioning system shall be designed to achieve at least 99.9% high-quality uptime from the perspective of end users. Uptime expectation excludes reasonable scheduled outages for upgrades, repairs, etc. as well as outages caused by factors outside of vendor control (such as KDE/school district network outages).
  - c. Vendor shall provide adequate functionality to detect and restrict DDOS attacks.
  - d. Vendor shall ensure that all components hosted by the vendor as part of the services are hosted in secure, reliable, redundant datacenters.

- e. Vendor shall identify any on-premises components or agents needed for overall system operation.
  - i. There shall be no on-prem components requiring VMs or hardware of any kind, past the retirement of on-prem Active Directory.
- 9. Vendor shall ensure that any interactive applications provided as part of the services (e.g., for administration, monitoring, configuration, etc.) that require user authentication also include appropriate session locking and session termination functionality.
- 10. Vendor shall comply with the relevant security regulations, privacy regulations, and best practices including but not limited to: Privacy Act of 1974, 5 U.S.C. 552a; the KY Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g); the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the KY Open Records Act, KRS 61.820 et seq.
- 11. Vendor shall work with KDE and other key partners to comprehensively validate functionality, capacity and performance in a test environment (including a vendor-provided test installation of their system) prior to general deployment and significant enhancements or changes.

## **B. Technical/Functional Requirements**

### **1. Provisioning**

- a. System shall be able to use Tyler Enterprise ERP (MUNIS) as an authoritative source Identity Authority (IdA) for K12 certified and classified staff.
  - i. System should be able to use the Tyler Enterprise ERP (MUNIS) as an authoritative source, identity authority (IdA), for K12 certified and classified staff, using Tyler's API approach.
  - ii. The system should provide the ability to write-back or provision to Tyler Enterprise ERP (MUNIS).
- b. System shall be able to use Infinite Campus as an authoritative source for K12 students.
- c. Vendor shall be prepared to reconfigure the system to continue functioning if the core authoritative sources change over time or are replaced.
- d. System shall provide a solution for users (for example, contract nurses, student teachers) that are not in either Tyler Enterprise ERP (MUNIS) or Infinite Campus (ex. Batch CSV import, manual entry in a vendor-

- provided portal). The system shall be able to act as an identity authority (IdA) under specific circumstances.
- e. The provisioning system shall be able to provision users from the authoritative sources to defined destination systems, currently Microsoft Active Directory (until its eventual retirement, forecasted for mid-2025 thru 2026), Microsoft 365, Google Workspace for Education, Clever (*for those districts utilizing it*), and any destination system that is certified for OneRoster 1.1 or newer.
  - f. This system shall replace upon implementation our current provisioning from legacy Active Directory to Microsoft 365 (Azure Active Directory Connect) as well as from legacy Active Directory to Google (Google Cloud Directory Sync - GCDS) for KDE and each school district. The system shall also have an interim solution with the current design until full implementation.
  - g. Solution should perform data cleansing by analyzing the source data, developing a balanced set of validation rules, and minimizing the opportunities for bad data to affect the provisioning process.
  - h. The solution should create Guest accounts for all K12 school district adults in KDE's Microsoft 365 tenant.
  - i. The system shall be capable of provisioning students from the KSD/KSB Infinite Campus instances into the Office 365 Tenant which is shared by KSD, KSB and other KDE Staff.
  - j. The system shall be able to manage the entire user life cycle (creation, update, disable, including provisioning and deprovisioning).
  - k. The solution shall be the authority for establishing user email addresses.
    - i. The solution should be able to provision the email address to MUNIS, Infinite Campus, and the other previously mentioned destinations.
  - l. The solution shall allow for individual district tailoring/configuration within the product (e.g., new provisioning to protocol-supported systems, changing the specific attributes that sync from authoritative source, etc.), if the configuration fits inside the statewide shared-service standards.
  - m. The solution shall allow individual districts to request provisioning customizations from the vendor, based on unique circumstances.
  - n. Solution shall support the OneRoster standard.
  - o. Solution should support the SCIM (System for Cross-domain Identity Management) protocol.
  - p. System should automatically place users in correct groups, using role- and attribute-based provisioning policies to add and remove access rights.



- q. Solution should allow configuration changes to be made centrally that can be distributed with minimal manual effort to meet requirements that affect all districts.
2. Authentication (IdP)
- a. The system shall act as the IdP for cloud-based systems, supporting at least the SAML and OpenID Connect protocols, and with proven integration as an IdP for Infinite Campus, Azure Active Directory (Microsoft Office 365 for Education), Google Workspace for Education and Clever.
  - b. The solution should have proven integration as an IdP for Tyler Enterprise ERP (MUNIS).
  - c. The solution shall provide adaptive Multi Factor Authentication options for both staff and students, with methods to include at least mobile app and SMS text.
  - d. The solution shall provide end-user Self-Service Password Reset with password writeback to Active Directory (until Active Directory eventual retirement).
  - e. The solution shall provide Conditional Access, including access based on geographical location, and the ability to refuse access or require additional authentication when meeting certain criteria.
    - i. The solution should include access filtering based on unknown devices, sensitive accounts, suspicious activity, and destination application.
  - f. The solution shall provide analytics and reporting capabilities to evaluate and alert identity risk.
  - g. The solution shall provide age and ability appropriate, platform agnostic (with the common platforms used in KY K-12 schools [Apple, Google, and Microsoft]), authentication methods and experience (K-12 focused).
    - i. The solution should allow for age and ability appropriate login to devices, including applications on the device, supporting devices with a variety of features such as fingerprint readers, cameras, NFC readers for the Chrome OS, current Windows operating systems, current MacOS platforms, and major mobile device operating systems. By way of example, a Chromebook user logs in to K12 Schools CUES IdP and gains access to device as if logging in natively.
  - h. The solution shall provide end-user notification of when passwords need to be changed. Expirations vary based on state and local district policy and procedure.
  - i. The solution should provide the ability for all users to authenticate using the WebAuthn protocol (FIDO2).
  - j. The solution shall provide phishing-resistant methods of authentication.

- k. The solution should provide an option for password-less authentication.
- l. The solution should provide a user self-service portal to allow for name changes, address changes, etc. with workflow for district administrator review and approval.
- m. The solution should provide scripting or API capabilities to allow districts to do ad-hoc or scheduled batch administration tasks.
- n. District shall have the ability to delegate to non-IT staff the ability to change student passwords (e.g., a teacher able to change the password of any of their students)
- o. Passwords must be stored using strong cryptographic hash functions.
- p. The system shall be able to provide a user dashboard or portal that provides easy access to a list of integrated and desired statewide and/or local district apps that can be customized by each district on a per-district basis.
- q. System should be capable of acting as a Relying Party to an external IdP, ideally with the ability to configure different external IdPs for different sets of users (e.g., personal consumer accounts for parents, etc.)
- r. Solution shall allow administrators to disable user accounts in such a way that existing authentication sessions including with relying party applications, can be expired quickly.
- s. Solution shall allow district administrators to manage the general configuration of the system for their district.
- t. Solution should allow configuration changes to be made statewide that can be distributed with minimal manual effort to meet requirements that affect all districts. (e.g. Applying security features to all users, adding a link to all staff dashboards.)
- u. Solution shall allow both districts and KDE to configure SSO relationships for applications (relying parties) that support the OIDC and/or SAML protocol without extra cost or IDP vendor involvement.

### **C. Monitoring, Reporting and Analysis**

This section contains requirements for monitoring and reporting on the health and activity of various components of the service.

- 1. Holistic service monitoring and alerting
  - a. Vendor shall proactively monitor the health of the entire service.
  - b. Vendor shall report service problems, regardless of component or layer, to KDE on a 24/7 basis using a consistent process.
  - c. Vendor shall report service problems, regardless of component or layer, to representatives of the specific districts affected on a 24/7 basis using a consistent process.

- d. Vendor should integrate problem alerts with KDE's overall health monitoring and alerting system by sending initial, ongoing status, and return to service alerts using a standard protocol; status updates should be provided at least hourly.
  - e. Vendor shall provide notifications to the KDE Customer Service Center and/or applicable local school district service center for unplanned outages within five (5) minutes of detection.
  - f. Vendor shall provide end-user notifications on account activity.
  - g. Vendor shall notify KDE Change Management and/or applicable local school district, through the KDE Customer Service Center and/or applicable local school district, a minimum of two (2) weeks prior to any planned outage.
  - h. Vendor shall provide a web-accessible portal allowing authorized KDE and district staff (district staff limited to their own district's data) to view the following:
    - i. Health of overall solution
    - ii. Health of each service (provisioning, IdP)
    - iii. Health of components and connections making up the solution
    - iv. Start time and duration of any current outage
2. Functional and Transactional Reporting
- a. System shall have a reporting feature per district which shows overall activity of IdP and provisioning, as well as granular reporting per identity (E.G. Why a user wasn't provisioned, How many users failed MFA authentication, etc.)
  - b. The Vendor shall have a documented, comprehensive strategy for achieving and reporting on service levels which covers the key deliverables of the overall solution and addresses cost adjustments.
  - c. The Vendor shall report on uptime and outages on a monthly basis or as requested by KDE. Reporting should reflect the availability of the service as a whole and per district.
3. Vendor shall provide reasonable methods of notification to all impacted school districts and KDE regarding service impacting issues.
4. Vendor should resolve any issues within four (4) business hours of diagnosis.
5. The system shall have rich monitoring and reporting capabilities for provisioning health. Ideally a dashboard for overall view of system health, only accessible by district level staff.

#### **D. Service and Support Delivery**

- 1. Vendor shall actively monitor and manage service components to ensure that they are not inappropriately out of date.

2. Vendor shall ensure that all services provided under contract are supported in a comprehensive, holistic manner and managed by a dedicated technical account manager.
3. Vendor shall provide districts the ability to configure end-user self-service and support details (e.g., Customized IdP splash screen, user specific support information)
4. Vendor shall provide access to support on provided services for KDE staff and district technology staff, through at least a toll-free phone line.
5. Vendor should provide support using U.S.-based staff who are fluent in the English language and have knowledge of the KY K-12 technology environment.
6. Vendor shall provide training, professional development, and knowledge base resources.
7. Vendor shall proactively engage district staff, through multiple channels and methods, to ensure districts continue to maximize benefits from the solution.
8. Vendor shall work with KDE staff to plan and schedule service changes (e.g., device replacements, software upgrades, etc.).
9. Vendor shall provide immediate notification for all unplanned outages to the KETS Service Desk.
10. Vendor shall notify OET Change Management, through the KETS Service Desk, a minimum of two (2) business days prior for any planned outages.
11. Vendor should, in collaboration with KDE, test and validate the performance of reliability mechanisms (e.g., failover) at least yearly.

## **E. Implementation**

1. Vendor shall provide a forecasted implementation plan with milestones to address all aspects below:
  - a. Core provisioning means that the system is provisioning basic user identity for all applicable persons (staff and students) to Google Workspace, Azure AD/Office 365, Clever, and legacy on-premise Active Directory; core authentication means that authentication is integrated for Google Workspace, Office 365, Clever, and all applications that are currently relying on those systems for authentication using a standard protocol (SAML and/or OpenID Connect).
2. Vendor shall be responsible for, working with KDE and each school district, the implementation of the solution to meet the functional requirements described in this document. Implementation activities will include:

- a. Creating and documenting an overall transition plan that allows for minimal downtime, and sufficient testing, proofs of concepts and piloting.
- b. Creating detailed design of the new solution, taking input from KDE and other key KETS partners, and documenting the detailed design.
- c. Creating and implementing training for technical staff, using multiple channels and methods, to ensure that all relevant district and KDE staff understand how to configure, administer, and maintain the solution. Training should be designed for both basic and advanced skillsets.
- d. Creating and documenting individual district transition plans, including scheduling site work in coordination with KDE and school district staff, capturing and analyzing existing configurations (per-district) in order to appropriately reimplement them, and creating documentation needed by KDE and district staff.
- e. Creating and documenting an operations plan, including any documentation needed by KDE and district staff for ongoing administration and use of the system.
- f. Executing the transition plans and validation of each district's successful implementation (both provisioning and authentication) in coordination with KDE technical and project management staff.
- g. Troubleshooting any issues with new services, in a holistic manner, until each district is stable.

### **3.2 Value-Added Services**

Value-added services, within scope of this Master Agreement, may be added to the contract with prior approval by the Commonwealth Office of Technology and the Office of Procurement Services Buyer of Record. Upon approval, a formal modification will be made to add the service(s). No work shall begin until a contract modification is completed and notice is provided by the OPS Buyer that work may begin.

## **SECTION 4 – COMMONWEALTH OFFICE OF TECHNOLOGY (COT) REQUIREMENTS**

#### **4.1 Hosting**

The system shall be hosted by the vendor, in a cloud-based secure, reliable, redundant datacenter. The vendor must align their security measures to the NIST 800-53 controls (at least, moderate level) and periodically assess themselves against them. FedRAMP moderate compliance or certification is preferred.

#### **4.2 Commonwealth Information Technology Policies and Standards**

- A. The vendor and any subcontractors shall be required to adhere to applicable Commonwealth policies and standards.
- B. The Commonwealth posts changes to COT Standards and Policies on its [Commonwealth Office of Technology - Home - Commonwealth Office of Technology \(Kentucky\)](#) website. Vendors and subcontractors shall ensure their solution(s) shall work in concert with all posted changes. Vendors or subcontractors that cannot comply with changes must, within thirty (30) days of the posted change, request written relief with the justification for such relief. The Commonwealth may: 1) deny the request, 2) approve an exception to the policy / standard, or 3) consider scope changes to the contract to accommodate required changes. Vendors or subcontractors that do not provide the response within the thirty (30) day period shall be required to comply within ninety (90) days of the change.

#### **4.3 Compliance with Commonwealth Security Standards**

The software deployment and all vendor services shall abide by privacy and security standards as outlined in the Commonwealth's Enterprise Information Technology Policies.

##### **Enterprise Security Policies**

<https://technology.ky.gov/OCISO/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx>

##### **Enterprise IT Policies**

<https://technology.ky.gov/policies-and-procedures/Pages/policies.aspx>

#### **4.4 Compliance with Industry Accepted Reporting Standards Based on Trust Service Principles and Criteria**

The vendor must employ comprehensive risk and threat management controls based on defined industry standards for service organizations such as ISO AICPA TSP section 100, Trust Services Principles and Criteria. The vendor must annually assert compliance and engage a third party certification registrar to examine such assertions and controls to provide a Report, such as ISO 9000, ISO 14001, AT101 SOC 2 type 2, on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy, which contains an opinion on whether the operating controls effectively support the

assertions. All such reports, including publicly available reports (i.e. AT 101 SOC 3) shall be made available to the Commonwealth for review.

#### **4.5 System Vulnerability and Security Assessments**

The Commonwealth reserves the right to conduct, in collaboration with the vendor, non-invasive vulnerability and security assessments of the software and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of these assessments, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls that will reduce risk to an acceptable and agreed upon level. An accredited third-party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

#### **4.6 Privacy Assessments**

The Commonwealth reserves the right to conduct Privacy assessments of the collection, use, maintenance and sharing of Commonwealth data by any vendor services, software, and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of this assessment, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls or privacy practices that will reduce risk to an acceptable and agreed upon level. An accredited third-party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

#### **4.7 Privacy, Confidentiality and Ownership of Information**

The Commonwealth is the designated owner of all Commonwealth data and shall approve all access to that data. The Vendor shall not have ownership of Commonwealth data at any time. The vendor shall not profit from or share Commonwealth data. The Vendor shall be in compliance with privacy policies established by governmental agencies or by state or federal law. Privacy notice statements may be developed and amended from time to time by the Commonwealth and will be appropriately displayed on the Commonwealth portal (Ky.gov). The Vendor should provide sufficient security to protect the Commonwealth data in network transit, storage, and cache. **All Commonwealth data, including backups and archives, must be maintained at all times**

**within the contiguous United States. All Commonwealth data, classified as sensitive or higher, as defined in Enterprise Standards, must be encrypted in-transit from Contractor's network and at rest while stored on Contractor's laptops or other portable media devices.**

#### **4.8 EU GDPR Compliance**

The Commonwealth of Kentucky requires all vendor contracts to comply to the extent applicable with the European Union's General Data Privacy Regulation [Regulation (EU) 2016/679] (the "GDPR") when the Commonwealth is a "controller" or "processor" of "personal data" from an individual "data subject" located in the European Union, as those terms are defined in the GDPR. The Contractor acknowledges and agrees that it is acting as a "processor" of "personal data" for the Commonwealth under this Agreement and that all applicable requirements of the GDPR are incorporated by reference as material terms of this Agreement. The Contractor represents and warrants that (1) it is aware of and understands its compliance obligations as a "processor" under GDPR; (2) it has adopted a GDPR compliant data privacy compliance policy/program, a summary of which has been provided to the Commonwealth; (3) it will process "personal data" only in accordance with the Commonwealth's instructions; and (4) with regard to its obligations under this Agreement, it shall comply with all applicable requirements of the GDPR. Additionally, the Contractor may be found liable to the Commonwealth for damages arising from any violation of applicable requirements of GDPR by the Contractor in its performance of the services hereunder, subject to Section 40.31, entitled Contractor's Limitation of Liability.

#### **4.9 X-as-a-Service Technical Definitions**

Refer to NIST 800-145

#### **4.10 Data Quality**

Vendor shall provide proposed levels of data quality per the following dimensions.

Data Quality is the degree to which data is valid, accurate, complete, unique, timely, consistent with all requirements and business rules, and relevant for a given use. The vendor shall provide data quality definitions and metrics for any data elements. Data has to be of the appropriate quality to address the needs of the Commonwealth of Kentucky. The following dimensions can be used to assess data quality:

- Validity – The data values are in an acceptable format.
- Accuracy – The data attribute is accurate.
- Completeness – There are no null values in a data field.
- Uniqueness – There are no duplicate values in a data field.
- Timeliness – The data attribute represents information that is not out-of-date.



- Consistency – The data attribute is consistent with a business rule that may be based on that attribute itself, or on multiple attributes.
- Adherence to business rules – The data attribute or a combination of data attributes adheres to specified business rules.

#### **4.11 Metadata Requirement**

The Vendor shall provide a glossary for all business terms used in this solution.

#### **4.12 Software Version Requirements**

All commercially supported and Commonwealth approved software components such as Operating system (OS), Database software, Application software, Web Server software, Middle Tier software, and other ancillary software must be kept current. In the event that a patch interferes with the solution, the vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution in to compliance to allow this patch to be applied in the shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

The Vendor shall keep software in compliance with industry standards to support third party products such as Java, Microsoft Edge, Mozilla Firefox, etc. at latest supported version, release, and patch levels, when such dependencies exist. In the event that a third party dependency interferes with the solution, the vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution into compliance to allow this third party dependency to be updated in the shortest timeframe possible, not to exceed three months, unless otherwise negotiated with the Commonwealth.

#### **4.13 No Surreptitious Code Warranty**

The Contractor represents and warrants that no copy of licensed Software provided to the Commonwealth contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this Contract as the "No Surreptitious Code Warranty".

As used in this Contract, "Self-Help Code" means any back door, time bomb, drop-dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access) for purposes of maintenance or technical support.

As used in this Contract, "Unauthorized Code" means any virus, Trojan horse, spyware, worm or other Software routines or components designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code.

In addition, Contractor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the Commonwealth.

The vendor shall defend the Commonwealth against any claim, and indemnify the Commonwealth against any loss or expense arising out of any breach of the No Surreptitious Code Warranty.

#### **4.14 Applicable Security Control Framework Compliance**

The vendor must have an awareness and understanding of the NIST Special Publication 800-53 Security Control Framework and employ safeguards that meet or exceed the moderate level controls as defined within the standard. The respondent must provide sufficient safeguards to provide reasonable protections around the Commonwealth's data to ensure that the confidentiality, integrity, and availability is maintained at an appropriate level. These include but are not limited to:

- *Access Control*

The vendor must employ policy and process that provide for stringent control to limit physical and logical access to systems that house Commonwealth data, on a need to know basis, provide clear separation of duties, and adheres to least privilege principles.
- *Awareness and Training*

The vendor must provide the appropriate role specific training for staff to ensure that there is awareness and understanding of roles and responsibilities as they relate to the protections around the Commonwealth's data.
- *Audit and Accountability*

There must be sufficient auditing capability to ensure that actions are tracked and there is individual accountability for all actions taken by vendor staff.
- *Configuration Management*

The vendor must work within established baselines that provide minimal functionality needed to ensure service delivery without exposing unnecessary risk. The vendor must also employ structured change control processes that provide a level of coordination with the client agreed upon in a Service Level Agreement (SLA).
- *Contingency Planning*

The vendor must employ contingent planning policy and procedures that ensure service delivery based on agreed SLA levels while maintaining all Commonwealth data within the continental United States.

- *Identification and Authorization*  
The vendor must employ appropriate identity and access management policies and procedures to ensure that access is appropriately authorized and managed at a level to ensure that access is provisioned and de-provisioned in a timely and efficient manner.
- *Incident Response*  
The vendor must employ policy and procedures to ensure that an appropriate response to all identified security incidents are addressed in a timely manner and are reported to the appropriate parties in an agreed upon SLA timeframe. The vendor must also ensure that all staff are sufficient trained to ensure that they can identify situations that are classified as security incidents.
- *Maintenance*  
The vendor must employ policy and procedures that ensure that all maintenance activities are conducted only by authorized maintenance staff leveraging only authorized maintenance tools.
- *Media Protection*  
The vendor must employ policy and procedure to ensure that sufficient protections exist to protect Commonwealth data on all storage media throughout the media lifecycle and maintain documentation from media creation through destruction.
- *Physical and Environmental Controls*  
The vendor must employ physical and environmental policies and procedures that ensure that the service and delivery infrastructure are located in a physically secure and environmentally protected environment to ensure the confidentiality, integrity, and availability of Commonwealth data.
- *Personnel Security*  
The vendor must employ policies and procedures to ensure that all staff that have access to systems that house, transmit, or process Commonwealth data have been appropriately vetted and have been through a background check at the time of hire and periodically thereafter.
- *System and Communications Protections*  
The vendor must employ physical and logical protection that protect system communications and communication media from unauthorized access and to ensure adequate physical protections from damage.

## SECTION 5 – PROCUREMENT REQUIREMENTS

### 5.1 Procurement Requirements

Procurement requirements are listed under “**Procurement Laws, Preference, Regulations and Policies**” and “**Response to Solicitation**” located on the eProcurement Web page at <https://finance.ky.gov/eProcurement/Pages/procurement-laws-regulations-and-policies.aspx>

and  
<https://finance.ky.gov/eProcurement/Pages/doing-business-with-the-commonwealth.aspx> respectively. The vendor must comply with all applicable statutes, regulations and policies related to this procurement.

5.2 **Omitted Intentionally**

5.3 **Omitted Intentionally**

5.4 **Omitted Intentionally**

5.5 **Confidentiality of Contract Terms**

The Contractor and the Commonwealth agree that all information communicated between them before the effective date of this Contract shall be received in strict confidence and shall not be necessarily disclosed by the receiving party, its agents, or employees without prior written consent of the other party. Such material will be kept confidential subject to Commonwealth and Federal public information disclosure laws.

Upon signing of this Contract by all parties, terms of the contract become available to the public, pursuant to the provisions of the Kentucky Revised Statutes.

The Contractor shall have an appropriate agreement with its subcontractors extending these confidentiality requirements to all subcontractors' employees.

5.6 **Omitted Intentionally**

5.7 **Omitted Intentionally**

5.8 **Omitted Intentionally**

5.9 **Omitted Intentionally**

5.10 **Omitted Intentionally**

5.11 **Omitted Intentionally**

**SECTION 9 – CONTRACT REQUIREMENTS AND PROVISIONS**

9.1 **Agencies to Be Served**

This Contract shall be for use by the **KENTUCKY DEPARTMENT OF EDUCATION AND ALL KENTUCKY PUBLIC K-12 SCHOOL DISTRICTS**. No shipments shall be made except upon receipt by vendor of an official delivery order from the using agency.

### **Extending the Contract Use to Other Agencies**

The Office of Procurement Services reserves the right, with the consent of the vendor, to offer this Master Agreement to other state agencies requiring the product(s) or service(s).

#### **9.2 Term of Contract and Renewal Options**

The initial term of the contract shall be for a period of **six (6) years** from the effective date of the Award of Contract.

This Contract may be renewed at the completion of the initial contract period for **five (5) additional one (1) year periods**. Such mutual agreement shall take the form of a contract modification as described in Section 10.7 of this Contract.

At the end of the Contract, the vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The vendor shall cooperate to this end with the vendor of the agency's choice, in a timely and efficient manner.

The Commonwealth reserves the right not to exercise any or all renewal options. The Commonwealth reserves the right to extend the contract for a period less than the length of the above-referenced renewal period if such an extension is determined by the Commonwealth Buyer to be in the best interest of the Commonwealth.

The Commonwealth reserves the right to renegotiate any terms and/or conditions as may be necessary to meet requirements for the extended period. In the event proposed revisions cannot be agreed upon, either party shall have the right to withdraw without prejudice from either exercising the option or continuing the contract in an extended period.

#### **9.3 Basis of Price Revisions**

**PRICE ADJUSTMENTS:** Unless otherwise specified, the prices established by this Contract shall remain firm for the contract period subject to the following:

- A. **Price Increases:** A price increase shall not occur during the first twelve (12) months of the contract. A vendor may request a price increase after twelve (12) months of the contract, which may be granted or denied by the Commonwealth. Any such price increase shall be based on industry wide price changes. The contract holder must request in writing a price increase at least thirty (30) days prior to the effective date, and shall provide firm proof that the price increase(s) is justified. The Office of Procurement Services may request additional information or justification. If the price increase is denied, the contract holder may withdraw from the contract without prejudice upon written notice and approval by the Office of Procurement Services. Provided,

however, that the vendor must continue service, at the contract prices, until a new contract can be established (usually within sixty (60) days).

- B. Price Decreases: The contract price shall be reduced to reflect any industry wide price decreases. The contract holder is required to furnish the Office of Procurement Services with notice of any price decreases as soon as such decreases are available.
- C. Extended Contract Periods: If the contract provides for an optional renewal period, a price adjustment may be granted at the time the contract is renewed, subject to price increase justification as required in Paragraph A "Price Increases" as stated above.

#### 9.4 Notices

All programmatic communications with regard to day-to-day performance under the contract are to be made to the agency technical contact(s):

**KDE Programmatic Contact:**  
**Chuck Austin**  
**Office of Education Technology**  
**300 Sower Blvd. 4<sup>th</sup> floor**  
**Frankfort, KY 46010**  
**[Chuck.Austin@education.ky.gov](mailto:Chuck.Austin@education.ky.gov)**  
**(502) 564-2020 X2231**

All communications of a contractual or legal nature are to be made to the Commonwealth Buyer:

**Susan S. Noland, KCPM**  
**Division Director**  
**COMMONWEALTH OF KENTUCKY**  
**FINANCE AND ADMINISTRATION CABINET**  
**Office of Procurement Services**  
**200 Mero Street, 5<sup>th</sup> Floor**  
**FRANKFORT KY 40622**  
**(502) 564-5951**  
**[Susan.Noland@ky.gov](mailto:Susan.Noland@ky.gov)**

#### 9.5 Subcontractors

The Contractor is permitted to make subcontract(s) with any other party for furnishing any of the work or services herein. The Contractor shall be solely responsible for performance of the entire contract whether or not subcontractors are used. The Commonwealth shall not be involved in the relationship between

the prime contractor and the subcontractor. Any issues that arise as a result of this relationship shall be resolved by the prime contractor. All references to the contractor shall be construed to encompass both the contractor and any subcontractors of the contractor.

## **SECTION 10 – STANDARD TERMS AND CONDITIONS**

### **10.1 Contract Components and Order of Precedence**

The Commonwealth's acceptance of the contractor's offer in response to the Solicitation RFP 758 2400000177, indicated by the issuance of a contract award by the Office of Procurement Services, shall create a valid contract between the Parties consisting of the following:

1. Procurement Statutes, Regulations and Policies
2. Any written Agreement between the Parties;
3. Any Addenda to the Solicitation RFP 758 2400000177;
4. The Solicitation RFP 758 2400000177 and all attachments
5. Any Best and Final Offer;
6. Any clarifications concerning the Contractor's proposal in response to the Solicitation RFP 758 2400000177;
7. The Contractor's proposal in response to the Solicitation RFP 758 2400000177.

In the event of any conflict between or among the provisions contained in the contract, the order of precedence shall be as enumerated above.

### **10.2 Final Agreement**

This Contract represents the entire agreement between the parties with respect to the subject matter hereof. Prior negotiations, representations, or agreements, either written or oral, between the parties hereto relating to the subject matter hereof shall be of no effect upon this Contract.

### **10.3 Contract Provisions**

If any provision of this Contract (including items incorporated by reference) is declared or found to be illegal, unenforceable, or void, then both the Commonwealth and the Contractor shall be relieved of all obligations arising under such provision. If the remainder of this Contract is capable of performance, it shall not be affected by such declaration or finding and shall be fully performed.

### **10.4 Type of Contract**

This Contract shall be on the basis of a **firm fixed unit price** for the elements listed.

### **10.5 Contract Usage**

The contractual agreement with the Vendor will in no way obligate the Commonwealth of Kentucky to purchase any services or equipment under this Contract. The Commonwealth agrees, in entering into any contract, to purchase only such services in such quantities as necessary to meet the actual requirements as determined by the Commonwealth.

**10.6 Addition or Deletion of Items or Services**

The Office of Procurement Services reserves the right to add new and similar items, by issuing a contract modification, to this Contract with the consent of the vendor. Until such time as the vendor receives a modification, the vendor shall not accept delivery orders from any agency referencing such items or services.

**10.7 Changes and Modifications to the Contract**

Pursuant to KRS 45A.210 (1) and 200 KAR 5:311, no modification or change of any provision in the contract shall be made, or construed to have been made, unless such modification is mutually agreed to in writing by the Contractor and the Commonwealth, and incorporated as a written amendment to the contract and processed through the Office of Procurement Services and approved by the Finance and Administration Cabinet prior to the effective date of such modification or change pursuant to KRS 45A.210(1) and 200 KAR 5:311. Memorandum of understanding, written clarification, and/or correspondence shall not be construed as amendments to the Contract.

If the contractor finds at any time that existing conditions made modification of the Contract necessary, it shall promptly report such matters to the Commonwealth Buyer for consideration and decision.

**10.8 Changes in Scope**

The Commonwealth may, at any time by written order, make changes within the general scope of this Contract. No changes in scope are to be conducted except at the approval of the Commonwealth.

**10.9 Contract Conformance**

If the Commonwealth Buyer determines that deliverables due under the contract are not in conformance with the terms and conditions of the contract and the mutually agreed-upon project plan, the Buyer may request the Contractor to deliver assurances in the form of additional contractor resources and to demonstrate that other major schedules will not be affected. The Commonwealth shall determine the quantity and quality of such additional resources and failure to comply may constitute default by the Contractor.

**10.10 Assignment**

This Contract shall not be assigned in whole or in part without the prior written consent of the Commonwealth Buyer.



**10.11 Payment**

The Commonwealth will make payment within thirty (30) working days of receipt of contractor's invoice or of acceptance of goods and/or services in accordance with KRS 45.453 and KRS 45.454.

Payments are predicated upon successful completion and acceptance of the described work, services, supplies, or commodities, and delivery of the required documentation. Invoices for payment shall be submitted to the agency contact person or his representative.

**10.12 Contractor Cooperation in Related Efforts**

The Commonwealth of Kentucky may undertake or award other contracts for additional or related work, services, supplies, or commodities, and the contractor shall fully cooperate with such other contractors and Commonwealth employees. The contractor shall not commit or permit any act that will interfere with the performance of work by any other contractor or by Commonwealth employees.

**10.13 Contractor Affiliation**

"Affiliate" shall mean a branch, division or subsidiary that is effectively controlled by another party. If any affiliate of the contractor shall take any action that, if done by the contractor, would constitute a breach of this agreement, the same shall be deemed a breach by such party with like legal effect.

**10.14 Commonwealth Property**

The Contractor shall be responsible for the proper custody and care of any Commonwealth-owned property furnished for contractor's use in connections with the performance of this Contract. The Contractor shall reimburse the Commonwealth for its loss or damage, normal wear and tear excepted.

**10.15 Confidential Information**

The Contractor shall comply with the provisions of the Privacy Act of 1974 and instruct its employees to use the same degree of care as it uses with its own data to keep confidential information concerning client data, the business of the Commonwealth, its financial affairs, its relations with its citizens and its employees, as well as any other information which may be specifically classified as confidential by the Commonwealth in writing to the Contractor. All Federal and State Regulations and Statutes related to confidentiality shall be applicable to the Contractor. The Contractor shall have an appropriate agreement with its employees, and any subcontractor employees, to that effect, provided however, that the foregoing will not apply to:

- A. Information which the Commonwealth has released in writing from being maintained in confidence;

- B. Information which at the time of disclosure is in the public domain by having been printed and published and available to the public in libraries or other public places where such data is usually collected; or
- C. Information, which, after disclosure, becomes part of the public domain as defined above, through no act of the contractor.

**10.16 Advertising Award**

The Contractor shall not refer to the award of contract in commercial advertising in such a manner as to state or imply that the firm or its services are endorsed or preferred by the Commonwealth of Kentucky without the expressed written consent of the buyer. (see Section 9.4)

**10.17 Patent or Copyright Infringement**

The Contractor shall report to the Commonwealth promptly and in reasonable written detail, each notice of claim of patent or copyright infringement based on the performance of this Contract of which the Contractor has knowledge.

The Commonwealth agrees to notify the Contractor promptly, in writing, of any such claim, suit or proceeding, and at the contractor's expense give the Contractor proper and full information needed to settle and/or defend any such claim, suit or proceeding.

If, in the Contractor's opinion, the equipment, materials, or information mentioned in the paragraphs above is likely to or does become the subject of a claim or infringement of a United States patent or copyright, then without diminishing the Contractor's obligation to satisfy any final award, the Contractor may, with the Commonwealth's written consent, substitute other equally suitable equipment, materials, and information, or at the Contractor's options and expense, obtain the right for the Commonwealth to continue the use of such equipment, materials, and information.

The Commonwealth agrees that the Contractor has the right to defend, or at its option, to settle and the Contractor agrees to defend at its own expense, or at its option to settle, any claim, suit or proceeding brought against the Commonwealth on the issue of infringement of any United States patent or copyright or any product, or any part thereof, supplied by the Contractor to the Commonwealth under this agreement. The Contractor agrees to pay any final judgment entered against the Commonwealth on such issue in any suit or proceeding defended by the Contractor.

If principles of governmental or public law are involved, the Commonwealth may participate in the defense of any such action, but no costs or expenses shall be incurred for the account of the contractor without the contractor's written consent.

The Contractor shall have no liability for any infringement based upon:

- A. the combination of such product or part with any other product or part not furnished to the Commonwealth by the Contractor.
- B. the modification of such product or part unless such modification was made by the Contractor.
- C. the use of such product or part in a manner for which it was not designed.

**10.18 Permits, Licenses, Taxes and Commonwealth Registration**

The Contractor shall procure all necessary permits and licenses and abide by all applicable laws, regulations, and ordinances of all Federal, State, and local governments in which work under this Contract is performed.

The Contractor shall maintain certification of authority to conduct business in the Commonwealth of Kentucky during the term of this contract. Such registration is obtained from the Secretary of State, who will also provide the certification thereof. Additional local registration or license may be required.

The Contractor shall pay any sales, use, and personal property taxes arising out of this Contract and the transaction contemplated hereby. Any other taxes levied upon this Contract, the transaction, or the equipment or services delivered pursuant hereto shall be borne by the Contractor.

**10.19 EEO Requirements**

The Equal Employment Opportunity Act of 1978 applies to All State government projects with an estimated value exceeding \$500,000. The contractor shall comply with all terms and conditions of the Act.

[Office of Equal Employment Opportunity and Contract Compliance - Finance and Administration Cabinet \(ky.gov\)](#)

**10.20 Provisions for Termination of the Contract**

This Contract shall be subject to the termination provisions set forth in 200 KAR 5:312.

**10.21 Bankruptcy**

In the event the Contractor becomes the subject debtor in a case pending under the Federal Bankruptcy Code, the Commonwealth's right to terminate this Contract may be subject to the rights of a trustee in bankruptcy to assume or assign this Contract. The trustee shall not have the right to assume or assign this Contract unless the trustee (a) promptly cures all defaults under this contract; (b) promptly

compensates the Commonwealth for the monetary damages incurred as a result of such default, and (c) provides adequate assurance of future performance, as determined by the Commonwealth.

**10.22 Conformance with Commonwealth & Federal Laws/Regulations**

This Contract shall be governed by and construed in accordance with the laws of the Commonwealth of Kentucky. Any action brought against the Commonwealth on this Contract, including but not limited to actions either for breach of contract or for enforcement of the contract, shall be brought in Franklin Circuit Court, Franklin County, Kentucky in accordance with KRS 45A.245.

**10.23 Accessibility**

Vendor hereby warrants that the products or services to be provided under this Contract comply with the accessibility requirements of Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, part 1194. Vendor further warrants that the products or services to be provided under this Contract comply with existing federal standards established under Section 255 of the Federal Telecommunications Act of 1996 (47 U.S.C. § 255), and its implementing regulations set forth at Title 36, Code of Federal Regulations, part 1193, to the extent the vendor's products or services may be covered by that act. Vendor agrees to promptly respond to and resolve any complaint regarding accessibility of its products or services which is brought to its attention.

**10.24 Access to Records**

The state agency certifies that it is in compliance with the provisions of KRS 45A.695, "Access to contractor's books, documents, papers, records, or other evidence directly pertinent to the contract." The Contractor, as defined in KRS 45A.030, agrees that the contracting agency, the Finance and Administration Cabinet, the Auditor of Public Accounts, and the Legislative Research Commission, or their duly authorized representatives, shall have access to any books, documents, papers, records, or other evidence, which are directly pertinent to this agreement for the purpose of financial audit or program review. The Contractor also recognizes that any books, documents, papers, records, or other evidence, received during a financial audit or program review shall be subject to the Kentucky Open Records Act, KRS 61.870 to 61.884. Records and other prequalification information confidentially disclosed as part of the bid process shall not be deemed as directly pertinent to the agreement and shall be exempt from disclosure as provided in KRS 61.878(1)(c).

**10.25 Prohibitions of Certain Conflicts of Interest**

In accordance with KRS 45A.340, the contractor represents and warrants, and the Commonwealth relies upon such representation and warranty, that it presently has

no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of its services. The Contractor further represents and warrants that in the performance of the contract, no person, including any subcontractor, having any such interest shall be employed.

In accordance with KRS 45A.340 and KRS 11A.040 (4), the Contractor agrees that it shall not knowingly allow any official or employee of the Commonwealth who exercises any function or responsibility in the review or approval of the undertaking or carrying out of this Contract to voluntarily acquire any ownership interest, direct or indirect, in the contract prior to the completion of the Contract.

**10.26 No Contingent Fees**

No person or selling agency shall be employed or retained or given anything of monetary value to solicit or secure this Contract, excepting bona fide employees of the offeror or bona fide established commercial or selling agencies maintained by the offeror for the purpose of securing business. For breach or violation of this provision, the Commonwealth shall have the right to reject the proposal or cancel this Contract without liability.

**10.27 Contract Claims**

The Parties acknowledge that KRS 45A.225 to 45A.290 governs contract claims.

**10.28 Limitation of Liability**

The liability of the Commonwealth related to contractual damages is set forth in KRS 45A.245.

**10.29 Discrimination**

Discrimination (because of race, religion, color, national origin, sex, sexual orientation, gender identity, age, or disability) is prohibited. This section applies only to contracts utilizing federal funds, in whole or in part. During the performance of this Contract, the Contractor agrees as follows:

1. The Contractor will not discriminate against any employee or applicant for employment because of race, religion, color, national origin, sex, sexual orientation, gender identity, or age. The Contractor further agrees to comply with the provisions of the Americans with Disabilities Act (ADA), Public Law 101-336, and applicable federal regulations relating thereto prohibiting discrimination against otherwise qualified disabled individuals under any program or activity. The Contractor agrees to provide, upon request, needed reasonable accommodations. The Contractor will take affirmative action to ensure that applicants are employed and that employees are treated during employment without regard to their race, religion, color, national origin, sex, sexual orientation, gender identity, age or disability. Such action shall include, but not be limited to the following; employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of

- pay or other forms of compensations; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this non-discrimination clause.
2. The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, religion, color, national origin, sex, sexual orientation, gender identity, age or disability.
  3. The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice advising the said labor union or workers' representative of the Contractor's commitments under this section and shall post copies of the notice in conspicuous places available to employees and applicants for employment. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance.
  4. The Contractor will comply with all provisions of Executive Order No. 11246 of September 24, 1965 as amended, and of the rules, regulations and relevant orders of the Secretary of Labor.
  5. The Contractor will furnish all information and reports required by Executive Order No. 11246 of September 24, 1965, as amended, and by the rules, regulations and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations and orders.
  6. In the event of the Contractor's noncompliance with the nondiscrimination clauses of this Contract or with any of the said rules, regulations or orders, this Contract may be cancelled, terminated or suspended in whole or in part and the contractor may be declared ineligible for further government contracts or federally-assisted construction contracts in accordance with procedures authorized in Executive Order No. 11246 of September 24, 1965, as amended, and such other sanctions may be imposed and remedies invoked as provided in or as otherwise provided by law.
  7. The Contractor will include the provisions of paragraphs (1) through (7) of section 202 of Executive Order 11246 in every subcontract or purchase order unless exempted by rules, regulations or orders of the Secretary of Labor, issued pursuant to section 204 of Executive Order No. 11246 of September 24, 1965, as amended, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions including sanctions for noncompliance; provided, however, that in the event a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such

direction by the agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

**10.30 Exception to Required Use of Contract**

The establishment of this Master Agreement is not intended to preclude the use of similar products when requested by the agency. The Commonwealth of Kentucky reserves the right to contract for large requirements by using a separate solicitation.

**10.31 Bidder, Offeror, or Contractor Mandatory Representations Compliance with Commonwealth Law**

The contractor represents that, pursuant to KRS 45A.485, they and any subcontractor performing work under this Contract will be in continuous compliance with the KRS chapters listed below and have revealed to the Commonwealth any violation determinations within the previous five (5) years:

KRS Chapter 136 (CORPORATION AND UTILITY TAXES)

KRS Chapter 139 (SALES AND USE TAXES)

KRS Chapter 141 (INCOME TAXES)

KRS Chapter 337 (WAGES AND HOURS)

KRS Chapter 338 (OCCUPATIONAL SAFETY AND HEALTH OF EMPLOYEES)

KRS Chapter 341 (UNEMPLOYMENT COMPENSATION)

KRS Chapter 342 (WORKERS' COMPENSATION)

**Boycott Provisions**

If applicable, the Contractor represents that, pursuant to KRS 45A.607, they are not currently engaged in, and will not for the duration of this Contract engage in, the boycott of a person or an entity based in or doing business with a jurisdiction with which Kentucky can enjoy open trade. **Note:** The term Boycott does not include actions taken for bona fide business or economic reasons, or actions specifically required by federal or state law.

If applicable, the Contractor verifies that, pursuant to KRS 41.480, they do not engage in, and will not for the duration of this Contract engage in, in energy company boycotts as defined by KRS 41.472.

**Lobbying Prohibitions**

The Contractor represents that they, and any subcontractor performing work under this Contract, have not violated the agency restrictions contained in KRS 11A.236 during the previous ten (10) years, and pledges to abide by the restrictions set forth in such statute for the duration of the contract awarded.

The Contractor further represents that, pursuant to KRS 45A.328, they have not procured an original, subsequent, or similar contract while employing an executive agency lobbyist who was convicted of a crime related to the original, subsequent, or similar contract within five (5) years of the conviction of the lobbyist.

10.31 **Insurance Requirements**

*\*\* Proof of all required insurances should be provided prior to award. \*\*  
A Certificate of Insurance (COI) on an ACORD form is preferred.*

The Vendor shall be responsible for maintaining this coverage through the entire contract term:

1. Commercial General Liability Insurance in accordance with limits of liability of \$1,000,000.00 per occurrence, \$2,000,000.00 aggregate

The Vendor shall furnish a Certificate of Insurance prior to award:

A. The certificate holder listed as:

Finance and Administration Cabinet, DCM  
Office of Procurement Services  
200 Mero Street, 5<sup>th</sup> Floor  
Frankfort, Kentucky 40622

B. Endorsement of Additional Insured

- Certificate of Insurance must contain the following language in the Description of Operations box, "The Commonwealth and its agents as an Additional Insured for this Contract. Additional insured protection afforded is on a primary and non-contributory basis."
- A copy of the Endorsement of Additional Insured must be submitted with the Certificate of Insurance.

C. Kentucky Department of Insurance and AM Best

- The insurance coverage shall be in compliance with the laws of the Commonwealth of Kentucky and shall be placed with a licensed resident or non-resident agent who represents insurance companies authorized to do business in Kentucky. A list of authorized companies can be found at <https://insurance.ky.gov/ppc/Company/Default.aspx>.
- The insurer shall have an AM Best rating of B+ or higher. Visit [www.ambest.com](http://www.ambest.com) for verification. Failure to meet this requirement may result in the bid being deemed non-responsive.



#### D. Subcontractors

If the contract allows for Subcontractors and utilizes Subcontractors, prior to the commencement of any work by a Subcontractor.

- The Subcontractor must submit and maintain a Certificate of Insurance that meets or exceeds the insurance requirements defined in this Contract or the Primary Contractor must submit a Certificate of Insurance identifying coverage on behalf of Subcontractor, with an Additional Insured Endorsement.
- OPS reserves the right to request copies of all Subcontractor's Certificate(s) of Insurance at any time.

All Certificates of Insurance must be signed by an authorized representative of the insurance agency. Proof of coverage on an Acord form is preferred. OPS reserves the right to request additional insurance documentation, if needed. Failure to furnish said certificates or failure to maintain the required coverage throughout the life of the awarded contract shall be grounds for cancellation of the contract.

#### Automobile Liability Insurance

Automobile Liability Insurance required for delivery. If the items requested in this Contract will be delivered by the awarded Contractor or Subcontractor, proof of Automobile Liability Insurance must be provided prior to award. ***If items will be delivered by common courier (USPS, FedEx, UPS, Old Dominion Freight Line, etc.), this requirement does not apply.***

Automobile Liability Insurance is also required for all on-site training, services, or events. If the Contractor or Subcontractor is required to drive on any Commonwealth property, Auto Liability Insurance is required.

#### Automobile Liability Insurance Requirements

The Contractor or Subcontractor must provide a certificate of insurance coverage for any vehicle used in performance of this Contract, whether owned, non-owned, or hired, or other vehicles utilized by the Contractor or Subcontractor. Said policy of insurance to have a minimum limit of \$1,000,000.00 per occurrence combined single limit for bodily injury, including death, and property damage. This paragraph does not apply if the Contractor does not own, lease, or hire any automobiles to be used in connection with performance under this Contract.

#### IV. Pricing

##### **Implementation Fees**

Milestone-based quarterly payment schedule for implementation and service cost.

Quarters are based on calendar year, Q1=January, Q2=April, Q3=July and Q4=October.

<b>Implementation Fees</b>		
<b>Payment Schedule</b>		
<b>Q3-24</b>	<b>\$100,000.00</b>	<b>Discovery, Assessment and Design Completion</b>
<b>Q4-24</b>	<b>\$100,000.00</b>	<b>Central Command Build &amp; District manifest Build completion</b>
<b>Q1-25</b>	<b>\$50,000.00</b>	<b>Prototype and POC completion; Pilot Phase underway</b>
<b>Q2-25</b>	<b>\$50,000.00</b>	<b>Begin District Rollout</b>
<b>Q3-25</b>	<b>\$75,000.00</b>	<b>District Rollout continuation</b>
<b>Q4-25</b>	<b>\$75,000.00</b>	<b>District Rollout continuation</b>
<b>Q1-26</b>	<b>\$75,000.00</b>	<b>District Rollout continuation</b>
<b>Q2-26</b>	<b>\$75,000.00</b>	<b>District Rollout completion</b>
<b>GRAND TOTAL Implementation</b>	<b>\$600,000.00</b>	

**Service Cost for RI Cloud Platform**

**All-inclusive Annual Enterprise Subscription cost based on total K-12 population (all staff, teachers, and students) to include all annual costs (management, support, licensing, infrastructure hosting costs, ongoing professional development, etc.) for all identified sites in Attachment C – Connected User Experience System Site List**

Quarters are based on calendar year, Q1=January, Q2=April, Q3=July and Q4=October.

<b>Remote Identity (RI) Cloud Platform Payment Schedule</b>	
<b>Q3-24</b>	<b>\$825,000.00</b>
<b>Q4-24</b>	<b>\$275,000.00</b>
<b>Q1-25</b>	<b>\$275,000.00</b>
<b>Q2-25</b>	<b>\$275,000.00</b>
<b>Q3-25</b>	<b>\$825,000.00</b>
<b>Q4-25</b>	<b>\$275,000.00</b>
<b>Q1-26</b>	<b>\$275,000.00</b>
<b>Q2-26</b>	<b>\$275,000.00</b>
<b>GRAND TOTAL RI Cloud Platform</b>	<b>\$3,300,000.00</b>

**Service Cost for RI Cloud Platform**

**All-inclusive Annual Enterprise Subscription cost based on total K-12 population (all staff, teachers, and students) to include all annual costs (management, support, licensing, infrastructure hosting costs, ongoing professional development, etc.) for all identified sites in Attachment C – Connected User Experience System Site List**

<b>Remote Identity (RI) Cloud Platform Payment Schedule</b>	
<b>Year 3</b>	<b>\$1,650,000.00</b>
<b>Year 4</b>	<b>\$1,650,000.00</b>
<b>Year 5</b>	<b>\$1,650,000.00</b>
<b>Year 6</b>	<b>\$1,650,000.00</b>
<b>Year 7 (Renewal Option 1)</b>	<b>\$1,732,500.00</b>
<b>Year 8 (Renewal Option 2)</b>	<b>\$1,819,125.00</b>
<b>Year 9 (Renewal Option 3)</b>	<b>\$1,910,081.00</b>
<b>Year 10 (Renewal Option 4)</b>	<b>\$2,005,585.00</b>
<b>Year 11 (Renewal Option 5)</b>	<b>\$2,105,865.00</b>

**Post Implementation Professional Services Hourly Rate – Maximum Not-to-Exceed Hourly Rate (all inclusive)**

<b>Year 1</b>	<b>\$250.00</b>
<b>Year 2</b>	<b>\$250.00</b>
<b>Year 3</b>	<b>\$250.00</b>
<b>Year 4</b>	<b>\$250.00</b>
<b>Year 5</b>	<b>\$250.00</b>
<b>Year 6</b>	<b>\$250.00</b>
<b>Year 7 (Renewal Option 1)</b>	<b>\$250.00</b>
<b>Year 8 (Renewal Option 2)</b>	<b>\$250.00</b>
<b>Year 9 (Renewal Option 3)</b>	<b>\$250.00</b>
<b>Year 10 (Renewal Option 4)</b>	<b>\$250.00</b>
<b>Year 11 (Renewal Option 5)</b>	<b>\$250.00</b>

**Value Added Services –**

<b>Security Manager</b> - Security Manager facilitates monitoring, analysis, and alerting regarding to identity activity and traffic.	<b>Not to exceed \$6.00 per Full Time Employee Count of the LEA (Local Education Agency) and KDE Annually</b>
<b>PhishID</b> - PhishID leverages AI Computer Vision to stop zero day phishing attacks at the point of click in the browser, regardless of where the phishing attempt begins.	<b>Not to exceed \$0.87 per user which includes Staff and Student Count of the LEA (Local Education Agency) and KDE Annual</b>


**V. Approvals**

This Contract is subject to the terms and conditions as stated. By executing this Contract, the parties verify that they are authorized to bind this agreement and that they accept the terms of this agreement.

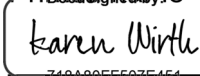
This Contract may be executed electronically in any number of counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same Contract.

This Contract is invalid until properly approved and executed by the Finance and Administration Cabinet.

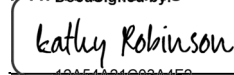
**1st Party: Identity Automation LP, as Contracting Agent (“Contractor”, “Vendor” or “IA”)**

Chris Honeycutt	CFO
_____ Printed name	_____ Title
<small>DocuSigned by:</small>  <small>ABECBB7FE8B64CF</small>	6/17/2024
_____ Signature	_____ Date

**2nd Party: Kentucky Department of Education, (“the Commonwealth”, “Customer” or “KDE”)**

Karen Wirth	Director
_____ Printed name	_____ Title
 <small>710A90FF507E451...</small>	6/17/2024
_____ Signature	_____ Date

**Approved by the Finance and Administration Cabinet  
Office of Procurement Services**

Kathy Robinson	Executive Director
_____ Printed name	_____ Title
 <small>12A54A21C03A4F2...</small>	6/17/2024
_____ Signature	_____ Date

**Attachments:**

**ATTACHMENT A – This Document**

**Revised ATTACHMENT B – Omitted Intentionally**

**ATTACHMENT C – Connected User Experience System Site List**

**ATTACHMENT D – Omitted Intentionally**

**ATTACHMENT E – The Protection of Personal Information Security and Breach Investigation Procedures and Practice Act (KRS 61.931)**

**ATTACHMENT F – Omitted Intentionally**

**ATTACHMENT G – Omitted Intentionally**

**ATTACHMENT H – KETS Technical Environment Overview**

**ATTACHMENT I – Omitted Intentionally**

**ATTACHMENT E**  
**Protection of Personal Information Security and Breach**

## Investigation Procedures and Practices Act

Vendors that receive Personal Information as defined by and in accordance with Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the "Act"), shall secure and protect the Personal Information by, without limitation, complying with all requirements applicable to non-affiliated third parties set forth in the Act.

"Personal Information" is defined in accordance with KRS 61.931(6) as "an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

- a) An account number, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
- b) A Social Security number;
- c) A taxpayer identification number that incorporates a Social Security number;
- d) A driver's license number, state identification card number or other individual identification number issued by an agency;
- e) A passport number or other identification number issued by the United States government; or
- f) Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by the Family Education Rights and Privacy Act, as amended 20 U.S.C. sec 1232g."

As provided in KRS 61.931(5), a "non-affiliated third party" means "any person or entity that has a contract or agreement with the Commonwealth and receives (accesses, collects or maintains) personal information from the Commonwealth pursuant to the contract or agreement."

The vendor hereby agrees to cooperate with the Commonwealth in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

The vendor shall immediately notify as soon as possible, but not to exceed seventy-two (72) hours, the contracting agency, the Office of Procurement Services, the Commonwealth Office of Technology and the NG-KIH Program Office of a determination of or knowledge of a breach, unless the exception set forth in KRS 61.932(2)(b)2 applies and the vendor abides by the requirements set forth in that exception.

The vendor hereby agrees that the Commonwealth may withhold payment(s) owed to the vendor for any violation of the Identity Theft Prevention Reporting Requirements.

The vendor hereby agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

Upon conclusion of an investigation of a security breach of Personal Information as required by KRS 61.933, the vendor hereby agrees to an apportionment of the costs of the notification, investigation, and mitigation of the security breach.

In accordance with KRS 61.932(2)(a) the vendor shall implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices established by the Commonwealth Office of Technology:

<https://technology.ky.gov/OCISO/Pages/InformationSecurityPolicies,StandardsandProcedures.aspx>



**Attachment C - Connected User Experience System Site List - MA 758 240000661**

<b>KDE (3)</b>
KDE
KY School for the Blind
KY School for the Deaf

<b>OET Test Sites (3)</b>
Harrodsburg Ind.
Monticello Ind.
Providence Ind.

<b>District (171)</b>
001 Adair County
005 Allen County
006 Anchorage Independent
011 Anderson County
012 Ashland Independent
013 Augusta Independent
015 Ballard County
016 Barbourville Independent
017 Bardstown Independent
021 Barren County
025 Bath County
026 Beechwood Independent
031 Bell County
032 Bellevue Independent
034 Berea Independent
035 Boone County
041 Bourbon County
042 Bowling Green Independent
045 Boyd County
051 Boyle County
055 Bracken County
061 Breathitt County
065 Breckinridge County
071 Bullitt County
072 Burgin Independent
075 Butler County
081 Caldwell County
085 Calloway County
091 Campbell County
092 Campbellsville Independent
095 Carlisle County

101 Carroll County
105 Carter County
111 Casey County
113 Caverna Independent
115 Christian County
121 Clark County
125 Clay County
131 Clinton County
132 Cloverport Independent
133 Corbin Independent
134 Covington Independent
135 Crittenden County
141 Cumberland County
143 Danville Independent
145 Daviess County
146 Dawson Springs Independent
147 Dayton Independent
149 East Bernstadt Independent
151 Edmonson County
152 Elizabethtown Independent
155 Elliott County
156 Eminence Independent
157 Erlanger-Elsmere Independent
161 Estill County
162 Fairview Independent
165 Fayette County
171 Fleming County
175 Floyd County
176 Fort Thomas Independent
177 Frankfort Independent
181 Franklin County
185 Fulton County
186 Fulton Independent
191 Gallatin County
195 Garrard County
197 Glasgow Independent
201 Grant County
205 Graves County
211 Grayson County
215 Green County
221 Greenup County
225 Hancock County
231 Hardin County
235 Harlan County
236 Harlan Independent
241 Harrison County

245 Hart County
246 Hazard Independent
251 Henderson County
255 Henry County
261 Hickman County
265 Hopkins County
271 Jackson County
272 Jackson Independent
275 Jefferson County
276 Jenkins Independent
281 Jessamine County
285 Johnson County
291 Kenton County
295 Knott County
301 Knox County
305 LaRue County
311 Laurel County
315 Lawrence County
321 Lee County
325 Leslie County
331 Letcher County
335 Lewis County
341 Lincoln County
345 Livingston County
351 Logan County
354 Ludlow Independent
361 Lyon County
365 Madison County
371 Magoffin County
375 Marion County
381 Marshall County
385 Martin County
391 Mason County
392 Mayfield Independent
395 McCracken County
401 McCreary County
405 McLean County
411 Meade County
415 Menifee County
421 Mercer County
425 Metcalfe County
426 Middlesboro Independent
431 Monroe County
435 Montgomery County
441 Morgan County
445 Muhlenberg County

446 Murray Independent
451 Nelson County
452 Newport Independent
455 Nicholas County
461 Ohio County
465 Oldham County
471 Owen County
472 Owensboro Independent
475 Owsley County
476 Paducah Independent
477 Paintsville Independent
478 Paris Independent
481 Pendleton County
485 Perry County
491 Pike County
492 Pikeville Independent
493 Pineville Independent
495 Powell County
501 Pulaski County
502 Raceland Independent
505 Robertson County
511 Rockcastle County
515 Rowan County
521 Russell County
522 Russell Independent
523 Russellville Independent
524 Science Hill Independent
525 Scott County
531 Shelby County
535 Simpson County
536 Somerset Independent
537 Southgate Independent
541 Spencer County
545 Taylor County
551 Todd County
555 Trigg County
561 Trimble County
565 Union County
567 Walton Verona Independent
571 Warren County
575 Washington County
581 Wayne County
585 Webster County
591 Whitley County
592 Williamsburg Independent
593 Williamstown Independent

595 Wolfe County
601 Woodford County

# Attachment H - MA 758 240000661

## KETS Technical Environment Information – Combined Documents

Last Reviewed: December 13, 2022

Last Updated: December 13, 2022

Active Directory-----	2
Internet Content Management System-----	6
Electronic Email and Collaboration -----	9
KETS Service Desk-----	15
MUNIS -----	19
The KEN Network (Kentucky Education Network) -----	23
Security-----	26
Infinite Campus Student Information System-----	30

The information contained within this Appendix is the current state for the respective Kentucky Educational Technology System (KETS) technical environments. Some environments refer to current or future project related work that may result in changes that impact the information contained within these documents. Where possible, that information is included. However, these documents are for high level planning purposes only.

The Kentucky Education Technology Systems (KETS) product and technology standards enable commonality and consistency among Kentucky's public school districts. These standards complement KETS initiatives and help ensure system supportability across all districts. While the technical environment described in this document follows these standards, the actual KETS Standards cover additional products and technologies, and new systems implemented at the state and district levels are expected to conform to these Standards where applicable. The KETS Standards can be found on the KDE website, currently at

<https://education.ky.gov/districts/tech/kpur/Pages/KETS%20Technology%20Standards%20and%20Purchasing.aspx>.

Department of Education  
Office of Education Technology  
Division of School Technology Planning and Project Management  
300 Sower Blvd.  
Frankfort, KY 40601  
(502) 564-2020

## **Active Directory**

### **Section 001**

Last Reviewed: 6/29/2022

Last Updated: 6/29/2022

Prepared by John Logan

Department of Education

Office of Education Technology

Division of School Technology Planning and Project Management

300 Sower Blvd.

Frankfort, KY 40601

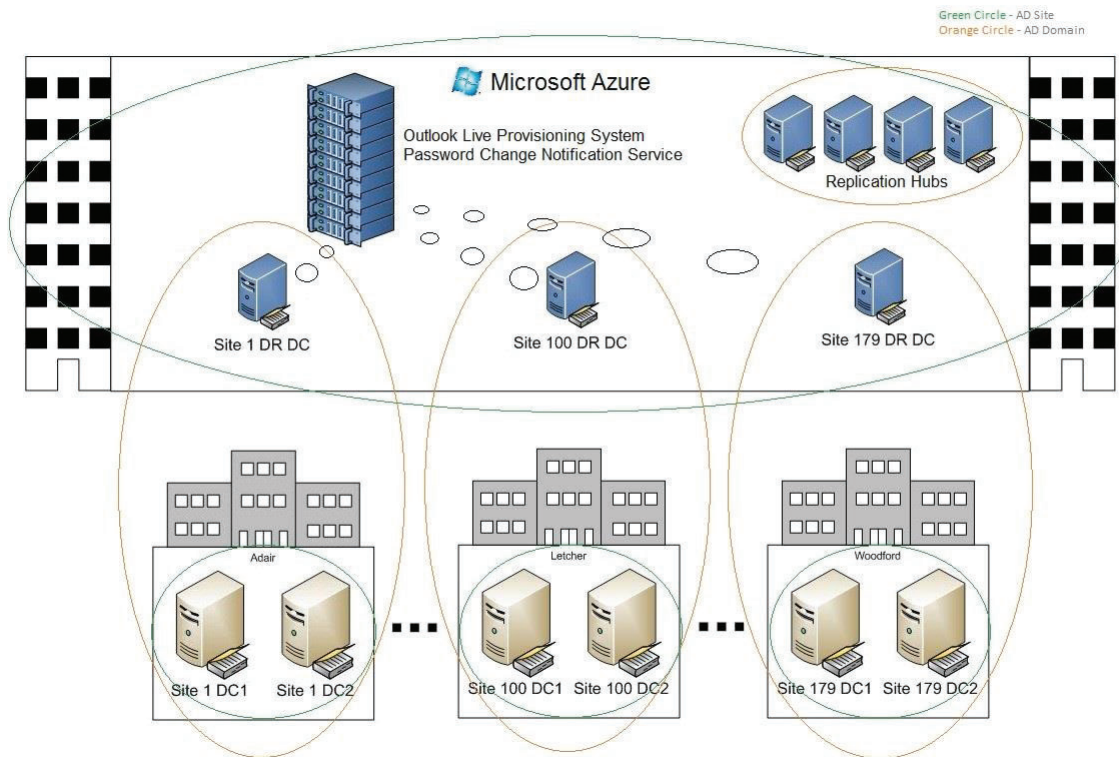
(502) 564-2020

## Summary

The KETS Active Directory provides authorization and authentication services for nearly 1,000,000 user objects and 500,000 computers and servers. It provides a directory structure for easier management of the user and computer objects throughout the KETS environment. Microsoft Active Directory services provide DHCP, DNS, WINS, Group Policies for object management, as well as normal directory services like authentication and authorization. There are also dependencies with our collaboration tools (Office 365 and G Suite) regarding account provisioning and password sync. Please visit Section 5 'Electronic Email and Collaboration' for more information.

## Visual Representation

This is a diagram of the KETS Active Directory structure. The green circles represent AD Sites for replication and the orange circles designate domains. One of the two district-located DCs is also a Global Catalog server. Though there are only three domains shown these represent 179 domains, and one empty root domain (180 total AD Domains). All Active Directory Domain Controllers are virtualized with the exception of the two root domain controllers located in Frankfort (GC/DC).





## Description

---

The KETS Active Directory is a mixed mode Windows Server single forest with 180 domains, averaging 3,500 users per domain. All domain controllers are running Windows Server. The smallest domain has approximately 500 users while the largest has nearly 125,000. The forest consists of a root domain, one domain each for the Department of Education, KY School for the Deaf (KSD), KY School for the Blind (KSB), a research and development domain as well as one domain for each of our 171 school districts. There are also three additional domains that are used for piloting updates. Each domain has a minimum of three domain controllers with one acting as a global catalog server. One DC for each domain is located in Microsoft Azure 'in the cloud'. This provides off-site redundancy from a district perspective. Generally, each district is also a single site within the directory structure. Replication within the forest is a hub and spoke model with replication hub servers hosted in Microsoft Azure and site links created between each domain and the hub site. AT&T's Netbond VPN solution as well as Microsoft ExpressRoute allow for a reliable network connection between the KETS on premise network and the cloud subnet.

Windows Server DNS provide naming services throughout the internal network. WINS is only enabled in a few districts. DHCP provides IP addresses to workstations while servers use static addressing.

Organizational units have been created within each district, named 'Students', 'Staff', 'Leadership', 'Workstations', and 'Local Servers'. These top-level organizational units cannot be deleted or have their permissions modified. Key district technical staff have been delegated permissions to create/modify child organizational units for each school in the district as prescribed in the KETS OU Naming Standards document (available upon request).

## Identity extends to O365 and G Suite for Education

---

Azure Active Directory Sync (AAD Sync) is configured for each school district, provisioning users and groups from on-prem Active Directory to each district's Office 365 tenant. These AAD Sync services are supported by KDE/OET. For those districts who have purchased Azure Active Directory Premium v1 they also have their passwords written back from O365 to on-prem AD, allowing for O365 Self Service Password Reset to be utilized.

G Suite Cloud Directory Sync (GCDS) is configured for some districts that choose to provision users and groups from on-prem Active Directory to their G Suite for Education tenant. This is supported by the school districts. There are some of these districts that also choose to have their passwords synchronized from on-prem AD provision to G Suite. For those districts OET has installed Google App Password Sync (GAPS) on the district AD Domain Controllers. This is supported by KDE/OET.

## **Management and Support Strategy**

---

The KETS Active Directory is monitored using Microsoft System Center Operations Manager. The KETS Messaging and Directory Services Team and the other operation service teams provide management of sites, site links, replication, domain controllers' hardware, and all naming services. The KETS Messaging and Directory Services Team manages all infrastructure and enterprise functions of Active Directory. District technical staff manage user account creation/modification, computer account creation/modification, and some group policy creation/modification within specified organizational units. Permissions have been delegated to a named group within each domain for these functions. When districts have issues they have the ability to call a technical service desk employed by KDE. Some issues are escalated to the KETS Messaging and Directory Service Team and potentially on to Microsoft through a Premier Support engagement.

**KETS Technical Environment Information Document**  
**Internet Content Management System**  
**(Previously: Application and Content Caching)**  
**Section 002**

---

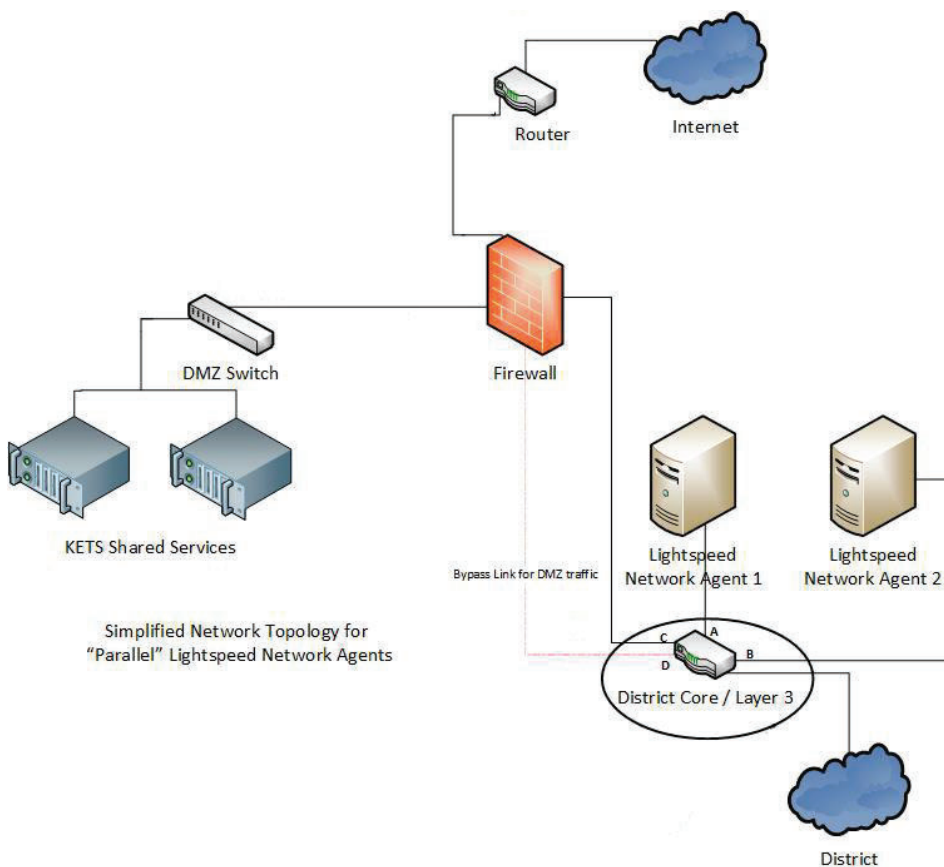
Created: June 23, 2005  
Last Reviewed: 06/15/2022  
Last Updated: 10/27/2021

Prepared By: Paul Shoemaker  
Department of Education  
Office of Education Technology  
Division of School Technology Planning and Project Management  
300 Sower Blvd.  
Frankfort, KY 40601  
(502) 564-2020

## Summary

This document describes the design and use of Internet Content Management Systems within the KETS or Kentucky Education Technology Systems network and within the districts.

## Visual Representation



## Description

The Kentucky Educational Technology System (KETS) utilizes an MPLS connection to the Internet. The districts and KDE the Agency have independent connectivity to the Internet through the MPLS cloud. KDE the Agency, as well as each school district, has their own independent Internet Management System based on the Lightspeed Relay product. Access and tracking are based on Active Directory authentication, IP addressing or client installation on the end-user system. This is a combination solution consisting of the Lightspeed Relay Smart Client used on district owned end user devices and the Network Agent used for all on premise devices not owned by districts (BYOD) or devices that cannot use the Relay Smart Agent software. Both solutions filter all Internet bound traffic

that pass through the Lightspeed Relay Smart Agent or Network Agent systems. The Lightspeed Relay Smart Agents and Network Agents are managed by the same administration console and policy sets and configurations are distributed to both systems. The Network Agent architecture is based on DNS requests to determine filtering policy application. The Network Agents are “Relay Aware” and do not filter devices that have the Relay Smart Agent installed.

Districts are allowed to request a waiver from the Lightspeed product and select their own Internet filtration device, so long as it meets the requirements documented in KAR 701-5:120, CIPA and other regulatory guidelines or statutes. A baseline configuration is provided to all districts that may be used as a guide with the Lightspeed system. Districts may alter that configuration to reflect any additional policies or restrictions they practice. Districts may employ a caching solution at their discretion.

## **Management Strategy**

---

The Office of Educational Technology (OET) provides the Lightspeed solution and a baseline configuration for all districts. Lightspeed provides direct support for this product for districts and KDE. Each district is responsible for their maintenance and configurations beyond the baseline provided. If a district has requested a waiver for a different product, the district is responsible for all support and configurations and is expected to arrange for support from the providing vendor.

# **KETS Technical Environment Information Document**

---

## **Electronic Email and Collaboration**

### **Section 003**

Last Reviewed: 6/29/2022

Last Updated: 10/28/2021

Prepared by John Logan

Department of Education

Office of Education Technology

Division of School Technology Planning and Project Management

300 Sower Blvd.

Frankfort, KY 40601

(502) 564-2020

## Summary

---

This document describes the electronic messaging and collaboration applications used by the Kentucky Department of Education, KSB, KSD, and the 171 Kentucky school districts. This comprises nearly 900,000 user mailboxes (faculty, staff and students).

These solutions are 'cloud-based' as backend systems that deliver these environments are maintained by the respective companies (Microsoft and Google). All districts and KDE have both a Office 365 and Gsuite for Education system. Each district/KDE choose where their users will use e-mail service specifically, but all other services are enabled for users (cloud drives, web conferencing, document sharing, etc). Users can choose which they want to use, but e-mail is enabled only for one of the systems for the entire districts or KDE.

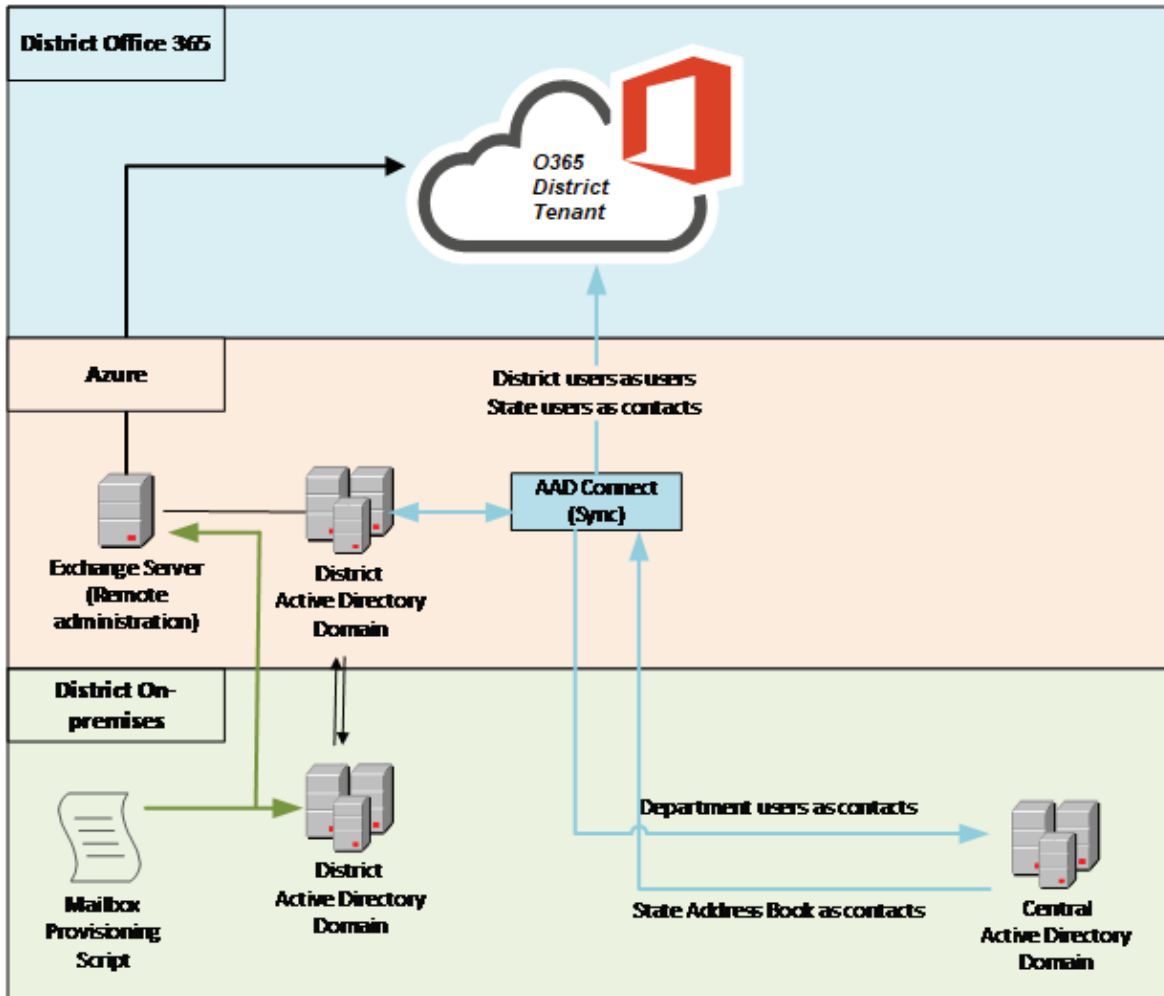
The Office of Education Technology manages the provisioning technologies to provision accounts to the Microsoft Office 365 environments. Districts/KDE manage provisioning to its own Google's Gsuite for Education environment. Districts and KDE maintain and manage their respective communications environment.

The provisioning of accounts (users, groups, etc.) is accomplished by Microsoft's Azure Active Directory Connector of Office 365 and Gsuite Cloud Directory Sync for Gsuite for Education. Both of these provisioning tools pull information from one Microsoft Active Directory environment. For a deeper understanding of our Active Directory environment you can go to that section in this document.

## Visual Representation

### Office 365 Provisioning

Visual representation Microsoft's provisioning topology as it pertains to Office 365



View of the provisioning infrastructure between Active Directory and Office 365. This allows us to utilize Active Directory for user management instead of using Office 365 directly for account creations, etc.

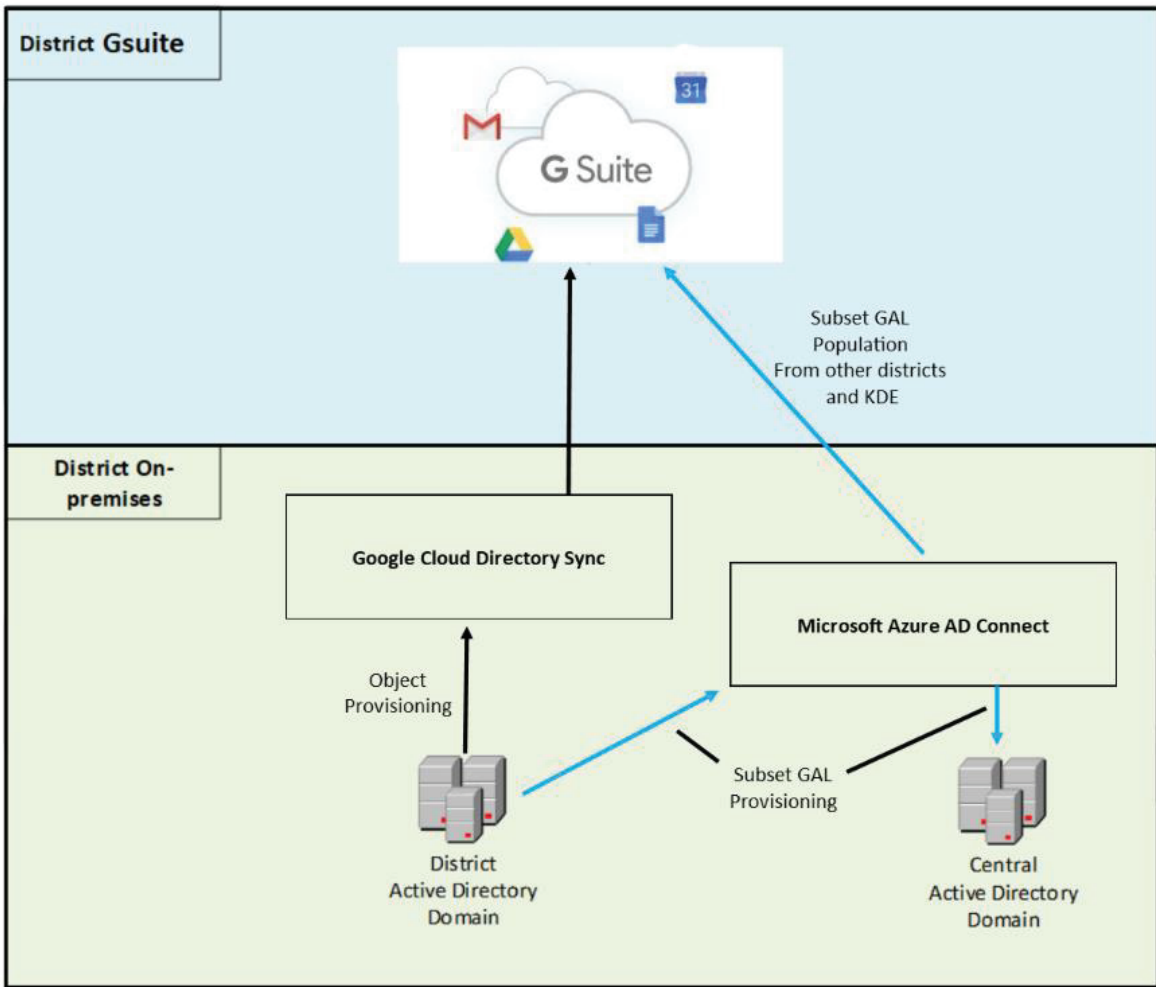


### SMTP Relay

There are 2 x Exchange Servers configure to forward SMTP email from allowed KETS devices (in districts and KDE). This is for devices that do not have the builtin ability to send email. By default all email sent through the relay goes out a single outbound connector, For those districts that wish to do DKIM Signing a dedicated connector is configured to their O365 or G Suite tenant where they can configure DKIM and then forward the mail.

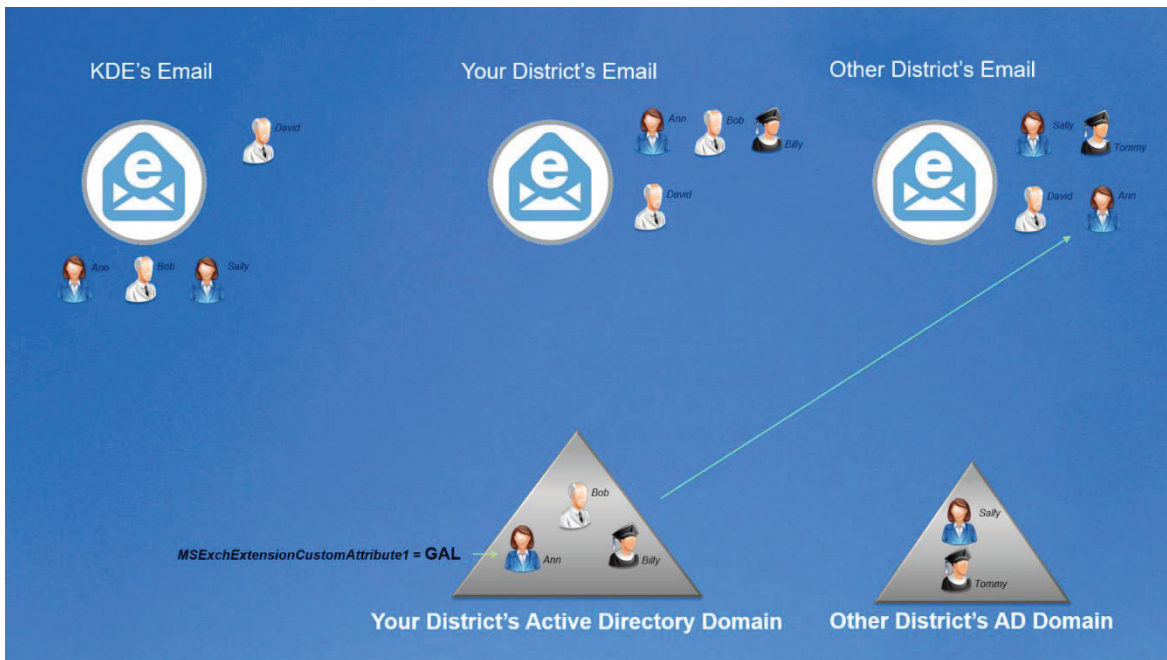
### Gsuite for Education Provisioning

Visual representation Google’s provisioning technologies as they pertain to Gsuite for Education



## Subset GAL

Visual representation how our 'Subset GAL' works



All adults in all districts show in KDE's Email Global Address list, and are also available to add to permissions of other Office 365 services (Sharepoint sites, OneDrive). Districts can add a value of GAL to a special attribute in Active Directory which will result in that user showing as a contact in all other district's email Global Address List.

## Description

---

The Office 365 solution is Microsoft's cloud collaboration offering provided out of Microsoft's datacenters. It is comprised of the following:

- Exchange Online – Microsoft's electronic messaging solution.
- Skype for Business / Teams – Microsoft's web-conferencing solution.
- SharePoint Online – Microsoft's organization solution for securely storing, organizing, sharing and accessing your information.
- OneDriveOnline – Microsoft's individual solution for securely storing, organizing, sharing and accessing your information.
- Office Professional Plus – Microsoft's cloud-deployed Office suite. This allows users to install and update the Office suite of tools on up to five devices from the Internet.

The Gsuite for Education solution is Google's cloud collaboration offering provided out of Google's datacenters. It is comprised of the following:

- Gmail – Google's electronic messaging solution.
- Google Meet – Google's web-conferencing solution.
- Google Drive – Google's individual solution for securely storing, organizing, sharing and accessing your information (Google doesn't have a like-product to Microsoft's SharePoint)
- Google Docs – Google's cloud productivity suite.

## Management Strategy

---

The KETS Messaging and Directory Services Team centrally manages the Active Directory and provisioning solution responsible for CRUD (creates, updates, deletes) between AD and Office 365. Districts manage those solutions for the Google environment. The backend infrastructures themselves are managed by Microsoft and Google respectively. When districts have issues they have the ability to call a technical service desk employed by KDE. Some issues are escalated to the KETS Messaging and Directory Service Team while many, depending on the issue, will be directed directly to Microsoft and/or Google or their support providers.

# **KETS Technical Environment Information Document**

---

## **KETS Service Desk**

### **Section 004**

Created: 6/24/2005

Last Reviewed: 7/08/2022

Last Updated: 1/28/2020

Prepared by Dan Gorman

Department of Education

Office of Education Technology

Division of School Technology Planning and Project Management

300 Sower Blvd.

Frankfort, KY 40601

(502) 564-2020

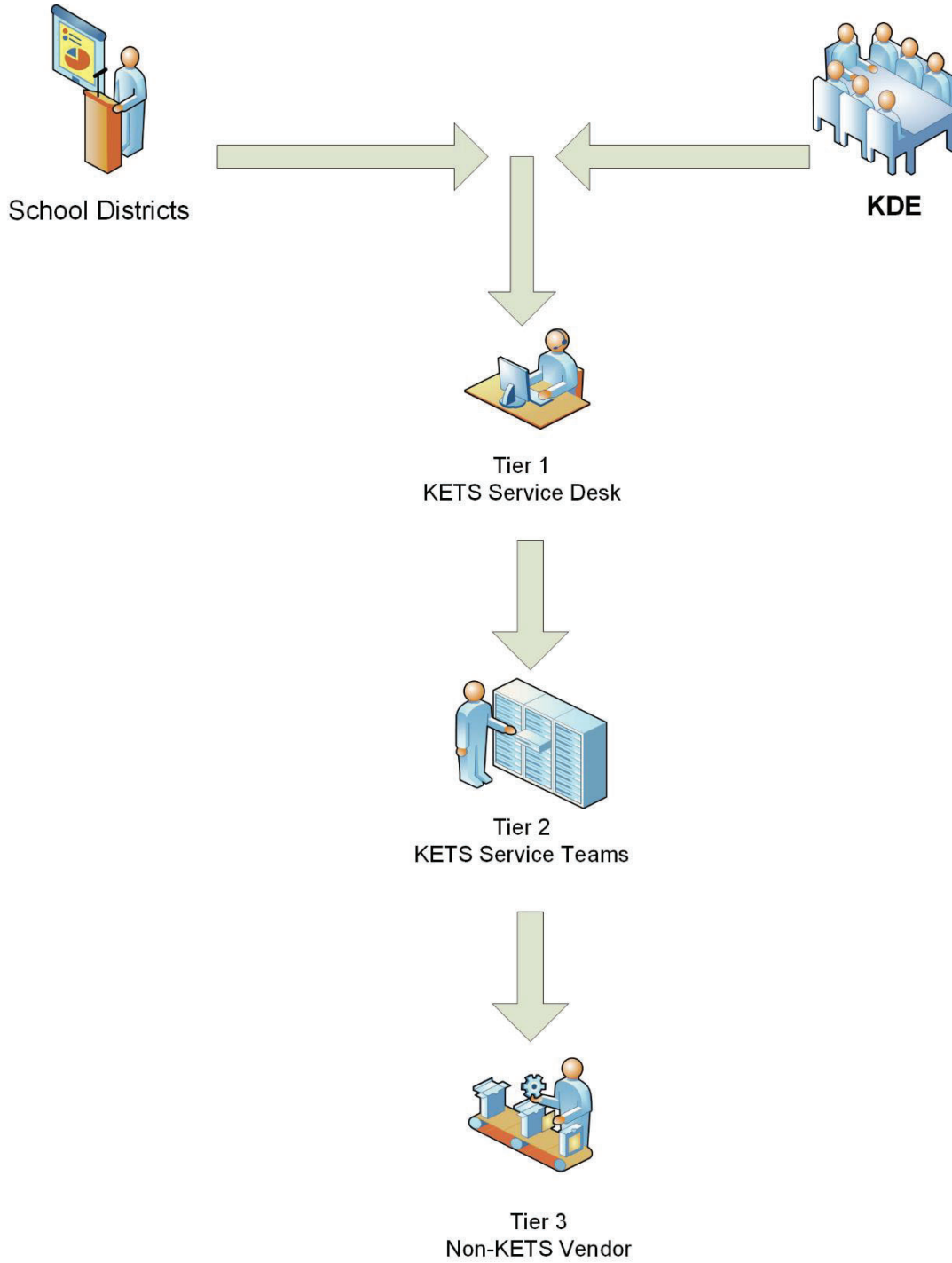
## **Summary**

---

This document provides an overview of the KETS Service Desk Services provided by the Office of Educational Technology.

# Visual Representation

---



## Description

---

The KETS Service Desk provides support to both internal and external KETS customers. Internal customers are defined as the Kentucky Department of Education (KDE) including the Kentucky School for the Blind (KSB) and the Kentucky School for the Deaf (KSD) as well as districts (171) and schools (approximate 1,400) throughout the state of Kentucky. The KETS Service Desk also services external customers defined as the general public who need assistance with any public facing technology that KDE provides such as web applications.

The KETS Service Desk resolves technical issues and answers questions on the following platforms and services: messaging, Internet/network connectivity, public facing web applications, internal end-user technology service (KDE the agency only), Active Directory, and network security. Issues are generally resolved within 20 minutes, though more complex issues may take longer. Resolution may entail working directly with a Service Desk analyst for a short time (Tier 1), escalation of an issue to another team within KETS (Tier 2), or by escalation to another non-KETS resource (Tier 3). Examples of a Tier 3 resource may include vendor partners such as Extreme, Microsoft, and McAfee.

Service provided to KDE the agency is often the first level of triage meaning that the Service Desk encounters a wide range of issues varying between simple password resets all the way to workstation reimages. Support provided to the school districts is often more technical in nature as the issues escalated to the KETS Service Desk have already gone through layers of technical support within the school district. However, this varies from district to district depending on the size and availability of IT staff. Issues escalated to the KETS Service Desk by school districts are either issues that can't be solved in the district or issues where the district staff may not have the rights to change something such as DNS entries or firewall configurations.

## Management Strategy

---

The KETS Service Desk is a process-driven entity and allows for seamless operation with KETS Service Teams. The KETS Service Desk is staffed each business day 7:30 AM – 5 PM Eastern. The KETS Service Desk is the central hub and entry point for accessing technical support for all KETS provided technology.

# **KETS Technical Environment Information Document**

---

## **Tyler Enterprise ERP (formerly MUNIS)**

### **Section 005**

Created: June 20, 2005

Last Reviewed: 6/21/2022

Last Updated: 6/21/2022

Prepared By Martin Herbener

Kentucky Department of Education

Office of Education Technology

Division of School Technology Planning and Project Management

300 Sower Blvd.

Frankfort, KY 40601

(502) 564-2020



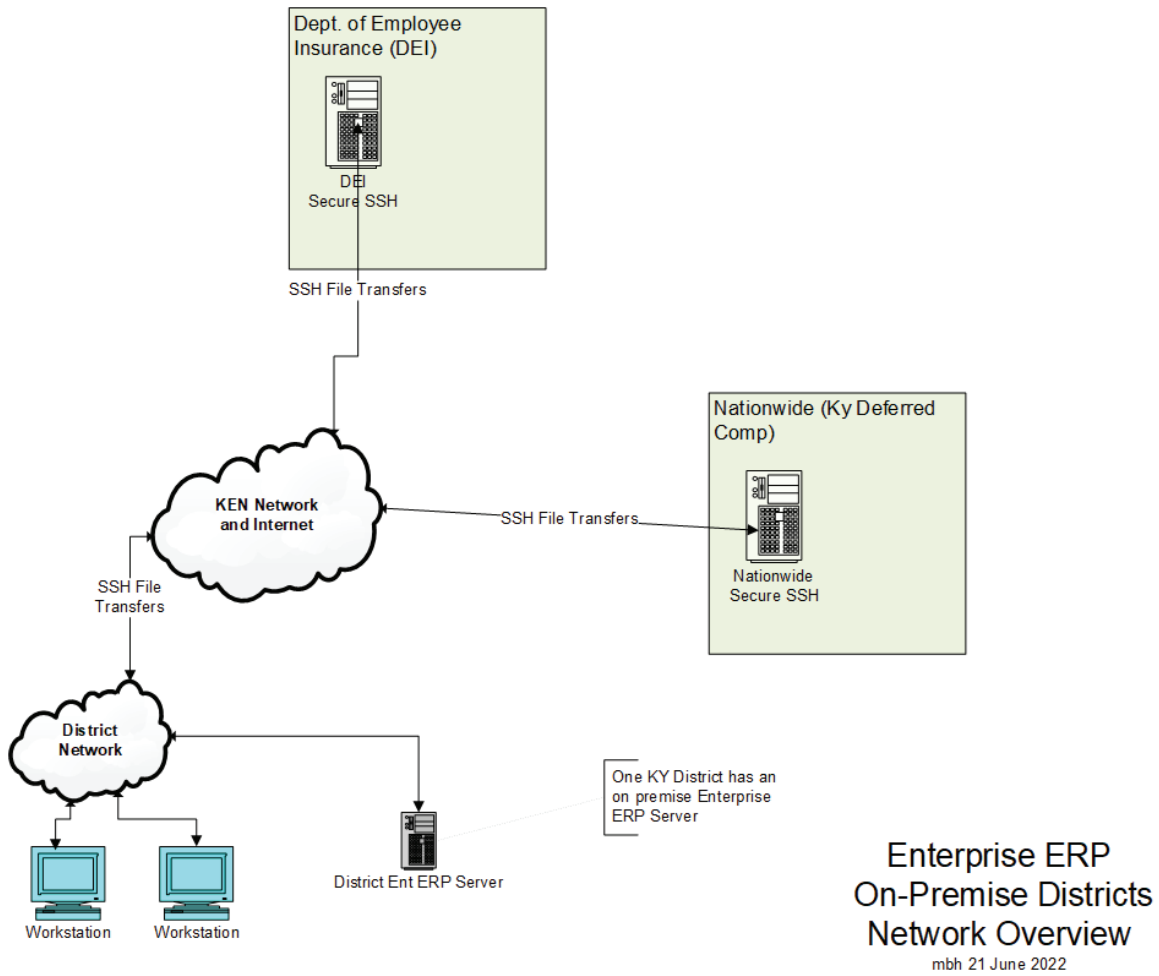
# Summary

This document covers Tyler Technologies' Enterprise ERP (formerly known as MUNIS), KETS's financial software.

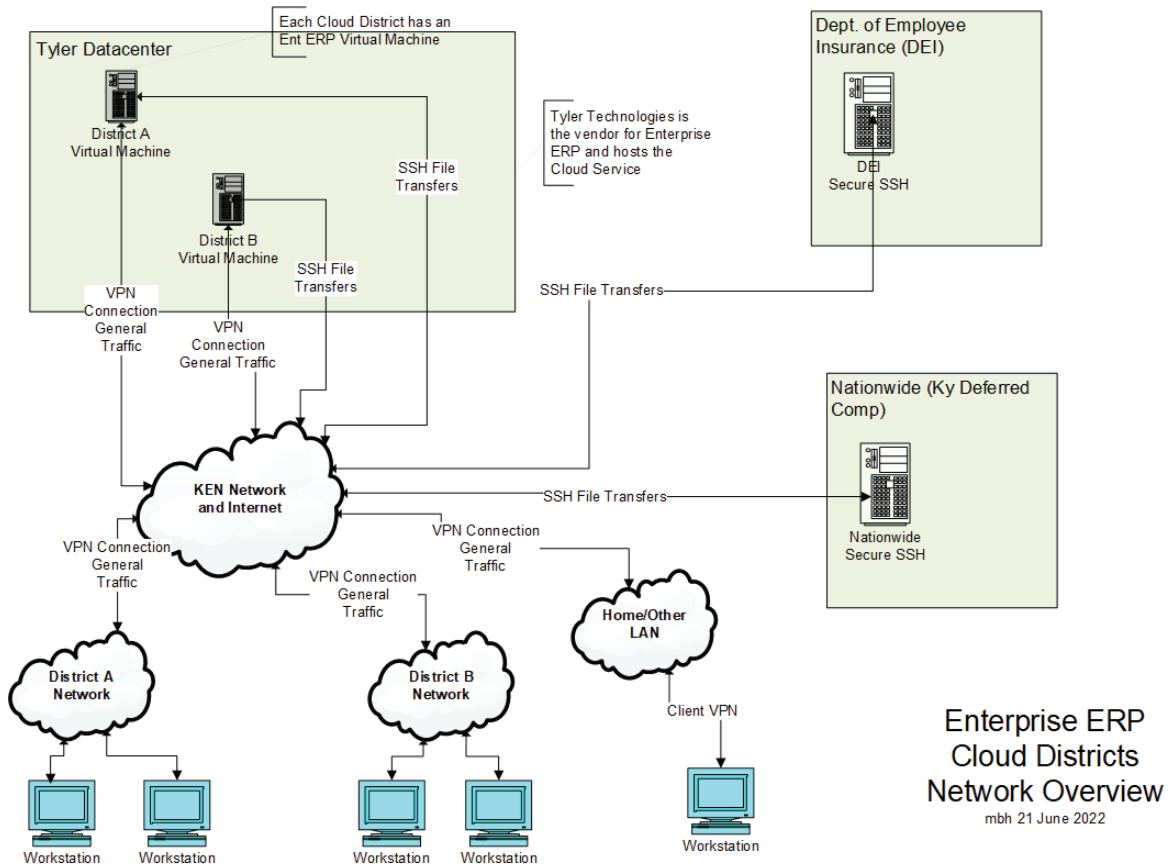
170 districts use a Cloud Service implementation; one district uses on-premise equipment. This document describes both implementations where applicable.

# Visual Representation

## 1.1. On-Premise Network Overview



## 1.2. Cloud Service Network Overview



### Description

Enterprise ERP (formerly known as MUNIS), from Tyler Technologies, is the financial system for Kentucky public school districts. For both the single remaining on-premise district and all Cloud districts it runs on Windows servers. Tyler Technologies hosts the Cloud districts in its own data centers. Most end user access requires connectivity to Tyler’s data centers through VPN; each district has a dedicated, Tyler-provided VPN device to provide this connectivity from computers on the district network, and Tyler also provides an end-user VPN service for user access from other locations.

Most functionality is browser-based, though a few specialized reporting features rely on additional client software. Tyler also maintains automated data transfers to and from the Commonwealth’s Department of Employee Insurance and Deferred Compensation vendor Nationwide.

Users are authenticated to both the end-user VPN (when used) and to the Enterprise ERP application using Enterprise ERP-specific credentials.

## **Management Strategy**

---

One remaining on-premise district in Kentucky has an Enterprise ERP server. Users, printers, security and operating system design are managed by the district with Tyler support.

For Cloud districts, users and printers are managed locally, while application updates, databases, security and the operating system are managed by Tyler.

KDE's Office of Finance and Operations provides policy guidance to districts regarding recording and reporting financial activities. KDE's Office of Education Technology provides oversight of technical operations and guides Kentucky-specific customizations of the system.

# **KETS Technical Environment Information Document**

## **The KEN Network (Kentucky Education Network)**

### **Section 006**

Last Reviewed 06/15/2022

Last Updated: 12/2/2021

Prepared by Howard Keeter

Reviewed by Paul Shoemaker

Department of Education

Office of Education Technology

Division of School Technology Planning and Project Management

300 Sower Blvd.

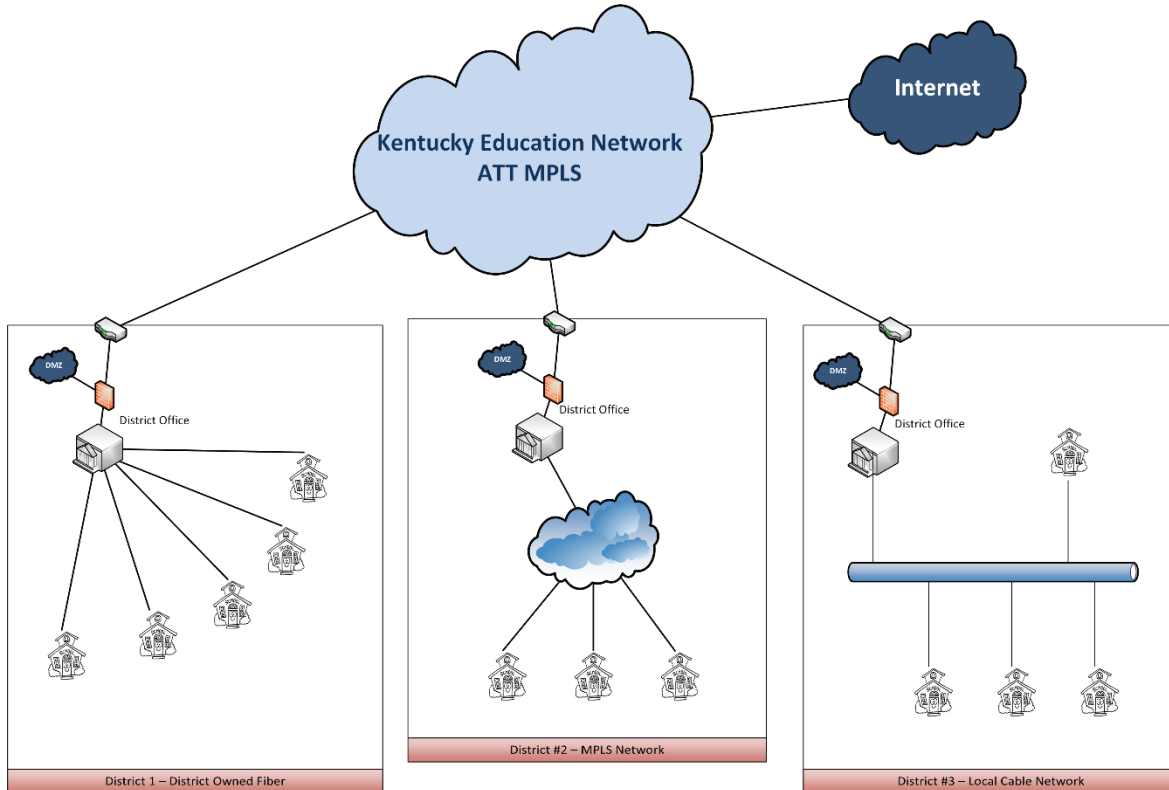
Frankfort, KY 40601

(502) 564-2020

## Summary

This document provides a brief, high-level view of the layout of the Kentucky Educational Technology System (KETS) networking environment throughout the Commonwealth of Kentucky. This document does not provide vendor-specific information with regard to network components, nor does it provide component level configuration information.

## Visual Representation



## Description

The Kentucky Education Network (KEN) network consists of 1200+ schools in 171 districts. There are over 1 million end user devices and servers serviced by KEN. Approximately 100,000 staff members and 650,000 students are consumers of the services of the network.

The current Kentucky Education Network consists of an MPLS backbone supplied by AT&T. The school districts have direct Internet connection via this MPLS backbone. Only services housed at a state level require connection to the Kentucky Department of Education. Each district connects to the backbone via an Ethernet hand off with lines speeds from 100Mb/s to 10Gb/s. At this district level the Kentucky Department of

Education supplies a managed firewall, traffic management device, and shared services switch solution. This is the demarcation point between the services supplied by the Kentucky Department of Education and district owned and managed services. In most cases the district connects to the managed firewall via a layer 3 switch or routing device. The buildings that make up the district connect to the district's hub site by any direct method that is available to them for that location. It cannot be assumed that all buildings in a district contain classrooms. Some examples of buildings with alternative uses are bus garages, athletic complexes, and technology and maintenance centers. The variety of connections can include methods such as District owned fiber or Managed Ethernet Services with line speeds from 100Mb/s to 10Gb/s. Inside each building there is at least one wiring distribution frame where the local Ethernet switches and additional components (such as phone systems and video distribution systems) are located. Classroom wiring is completed as homeruns back to these wiring distribution frames. Wiring between distribution frames inside a building is generally completed by the use of multi-mode fiber optic cable. If wiring is needed between buildings on a campus it is encouraged that it be done with the use of single mode fiber optic cable.

## **Management Strategy**

---

The Office of Educational Technology, with the assistance of vendor partners, supports and maintains all centralized KETS shared service level and distributed components, including Firewalls, VPN servers, Traffic Management devices, etc. for all 171 school districts. Additionally, all hardware components, Leased-Line connectivity, and configuration management for connectivity between the school district's hub site and the state is funded and managed by OET. OET sets standards for all other network-related components and negotiates contracts on behalf of the school districts with approved vendors. OET also provides design and configuration assistance to school districts on an as-needed basis. School districts are responsible for all networking components and their configuration and management within their own LANs on their side of the KETS Firewall.

# **KETS Technical Environment Information Document**

---

## **Security**

### **Section 007**

Created: June 22, 2005

Last Reviewed: 06/15/2022

Last Updated: 10/27/2021

Prepared By Paul Shoemaker

Department of Education

Office of Education Technology

Division of School Technology Planning and Project Management

300 Sower Blvd.

Frankfort, KY 40601

(502) 564-2020

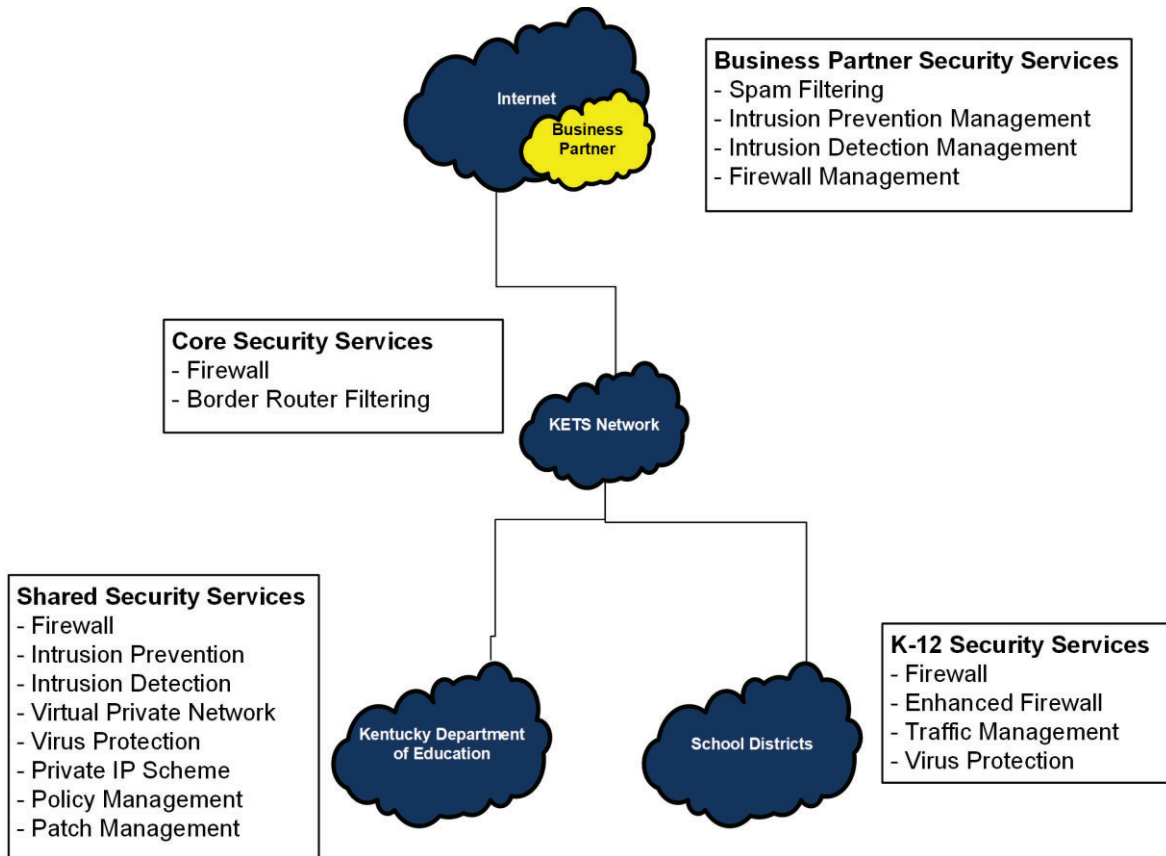
## Summary

---

This document provides an overview of the Network Security Services provided by the Office of Educational Technology (OET) for the Kentucky Educational Technology System (KETS). This document only covers security services supported by the OET Network Security Team and Contracted Network Management Services with AT&T Network Services.

## Visual Representation

---





## Description

---

Network Security Services include the following:

1. Intrusion Detection – Systems that passively monitor and detect harmful network traffic or attacks
2. Border Router Filtering – Basic filters placed on border routers which filter out common “noise” before it hits security devices
3. Firewall Services – Systems that provide security of outward facing network connections.
4. Enhanced Firewall – Additional protection for end user devices when connecting to outside networks.
5. SPAM Filtering – Systems that monitor and remove unwanted e-mail sent to the KETS network
6. Intrusion Prevention – Systems that actively look for harmful network traffic or attacks and reset connections as needed
7. Virtual Private Networking – Systems that allow secured access to the KETS Network from outside networks
8. Virus Protection – Virus detection and removal software that is loaded on all workstations and servers in the KETS network
9. Traffic Management – Systems that can either guarantee or limit the amount of traffic of any specific type on the network
10. Certificate Services (Internal usage only) – A root certificate authority tied to the KETS AD forest is established at KDE. Districts wanting to implement certificate services may stand up their own subordinate certificate server to be used for wireless authentication and other certificate related authentication practices required in the district
11. Policy Management – Baseline rule sets for firewalls, virus protection, VPN, and other security-related systems
12. Patch Management – Systems that monitor status of and install patches to operating systems and other software within the KETS network
13. Private IP Scheme – Standardized assignment of Private Internet Protocol addresses to devices within the KETS network, as well as Network Address Translation to allow some of these devices to interact with the Internet

## Management Strategy

---

Intrusion Detection, Firewall Services, Enhanced Firewall services, SPAM Filtering, Intrusion Prevention, Traffic Management, and Virtual Private Networking are all managed by a combination of the OET Network Security Team, Microsoft Office365 and Contracted Network Management Services (AT&T). Policy Management is managed by a combination of the OET Network Security Team and relevant vendors. Border Router Filtering is cooperatively managed by the OET Network Security Team and AT&T Network Services and Contracted Network Management Services with AT&T Network Services that handle daily maintenance and updates while the OET Network Security Team handles defining policies. Virus Protection, Patch Management, and Private IP are supported by both the Network Security Team and local district support. Certificate services are granted to districts’ subordinate certificate servers through KDE. Districts

issue, expire and reclaim certificates to their end users through their own support local support services.

# **KETS Technical Environment Information Document**

---

## **Infinite Campus Student Information System**

### **Section 008**

Created: February 23, 2009

Last Reviewed: 6/21/2022

Last Updated: 10/26/2021

Prepared By Martin Herbener

Department of Education

Office of Education Technology

Division of School Technology Planning and Project Management

300 Sower Blvd.

Frankfort, KY 40601

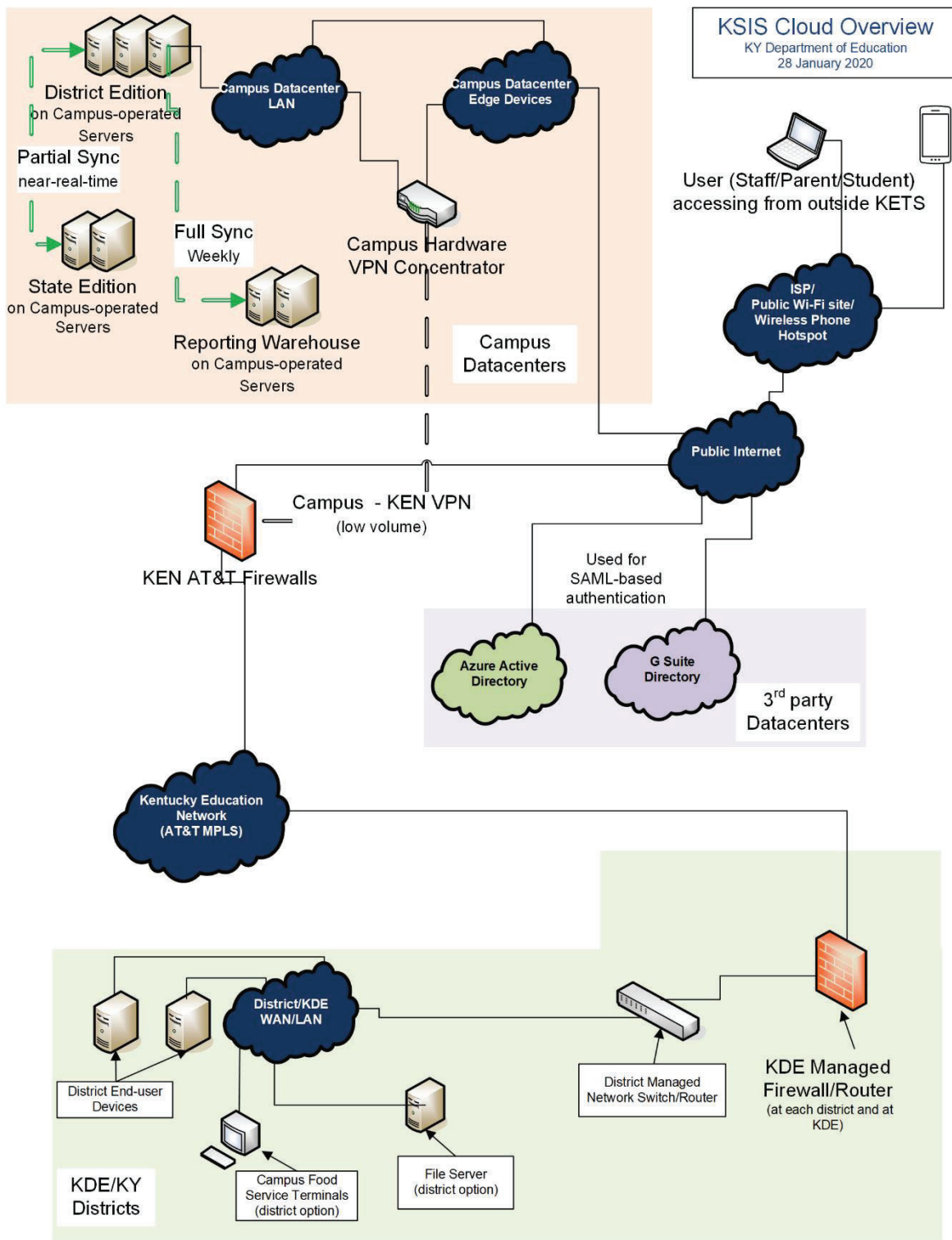
(502) 564-2020

## Summary

---

The Kentucky Student Information System (KSIS), based on Infinite Campus, is the system of record for most student-level data for all public school districts across Kentucky and allows districts and KDE to create reports for decision-making purposes. KSIS is cloud-based (hosted by Infinite Campus) for all districts and for the state-level components using a Software as a Service model.

# Visual Representation



## Description

---

Infinite Campus provides the KETS standard student information system. This system includes three main components:

- Infinite Campus District Edition
- Infinite Campus State Edition
- Statewide Reporting Warehouse

Plus two optional (per-district) components:

- Food Service
- Messenger with Voice

**Infinite Campus District Edition** is the application used by school and district staff – teachers, administrators, and support staff. It tracks data such as attendance, grades, behavior, student demographics, schedules, fees, instructional plans, and health. It produces numerous reports and constantly synchronizes certain data elements with the centralized Infinite Campus State Edition installation. As a web-based application it is accessible anywhere in the district and from the general Internet. Campus Student and Campus Parent interfaces, with accompanying mobile apps, are available for those populations to use.

**Infinite Campus State Edition** is the application used by KDE and other state-level staff. It automatically receives certain data elements from each District Edition installation for reporting purposes. It is also used to manage district, school, and in rare cases (such as duplicate student ID cleanup) student records.

The **State Reporting Warehouse** is a single SQL Server database instance which contains copies of all the Infinite Campus District Edition databases, updated weekly. This database is used as the source for reports that required detailed data which are not synchronized to the Infinite Campus State Edition application.

**Infinite Campus Food Service** is an optional module that manages cafeteria menus and links with Point of Sale devices to process food service transactions.

**Infinite Campus Messenger with Voice** is an optional module that places voice phone calls and/or SMS (text) messages to staff, students and/or parents based on triggers (such as absences) or manual input (such as to announce special events).

## Management Strategy

---

The Kentucky Student Information System based on Infinite Campus is operated as a service provided by Infinite Campus. Infinite Campus owns, monitors and administers all equipment other than Point of Sale terminals. AT&T (on behalf of KDE) is responsible for the network infrastructure used by districts to connect to the Internet, while districts are responsible for their local networks, client devices, and Point of Sale terminals. A dedicated VPN connection between the KETS and Infinite Campus networks, which is used for a limited set of data transfers, is jointly managed by Infinite Campus and AT&T.